VIRTUAL ACCESS

SMART NETWORK SOLUTIONS
FOR SERVICE PROVIDERS

GW6600 User Manual

Issue: 2.3

Date: 08 May 2015

1 Introduction 10
1.1 Document scope 10
2 GW6600 Series hardware 11
2.1 Hardware specification 11
2.1.1 GW6600 Series router model variants 11
2.2 Hardware features 11
2.3 GSM technology 11
2.4 Power supply 12
2.5 Dimensions 12
2.6 Compliance 12
2.7 Operating temperature range 12
2.8 Antenna 12
2.9 Components 12
2.10 Inserting the SIM cards 13
2.11 Connecting the SIM lock 14
2.12 Connecting cables 14
2.13 Connecting the antenna 14
2.14 Connecting the WiFi antenna 14
2.15 Powering up 14
2.16 Reset button 14
3 GW6600 Series LED behaviour 16
3.1 Main LED behaviour 16
3.2 Ethernet port LED behaviour 18
4 Factory configuration extraction from SIM card 19
5 Accessing the router 20
5.1 Over Ethernet 20
5.2 Over a 3G or 4G interface 20
6 Upgrading router firmware 21
6.1 Upgrading firmware using the web interface 21
6.2 Upgrading firmware using CLI 23
7 File system 24
7.1 Configurations 24
7.1.1 High level configuration commands 24
7.1.2 Configuration file syntax 25
7.1.3 Command line utility 26
7.1.3.1 Command line utility examples 28
7.1.4 Configuration copying and deleting 29
7.1.5 Image files 29
7.1.6 Viewing files 29
7.1.7 Copying files 30

7.1.8 Editing files 31
7.1.9 Processes and jobs 31
7.1.10 System information 31
8 Command Line Interface 33
8.1 Basics 33
8.2 Unified Configuration Interface (UCI) 35
8.3 Configuration files 39
8.4 Configuration file syntax 39
8.5 Examples 40
8.5.1 Export an entire configuration 41
8.5.2 Display just the value of an option 41
9 Management configuration settings 42
9.1 Autoload - boot up activation 42
9.2 Httpclient - Activator configuration 44
9.3 System settings 47
9.3.1 Configuring a router's host name 47
9.4 User management 50
9.4.1 Configuration file: config user 50
9.4.2 UCI export and UCI show commands 52
9.5 Interfaces configuration 53
9.5.1 Interfaces 53
9.5.2 Options valid for all protocol types 54
9.5.3 Protocol "static" 55
9.5.4 Protocol "dhcp" 55
9.5.5 Protocol "3g" (PPP over EV-DO, CDMA, UMTS or GRPS) 55
9.5.6 Protocol "l2tp" (layer 2 tunneling protocol) 56
9.5.7 Aliases 56
10 DHCP server and DNS configuration 59
10.1 Common options section 59
10.2 DHCP pools 63
10.3 Static leases 65
11 VLAN configuration 66
11.1 VLAN web interface 66
11.2 VLAN definition 66
11.3 Port description 67
11.4 VLANs UCI interface 68
11.4.1 config port 70
11.4.2 config vlan 70
11.4.3 Config nat vlan 70
12 Static routes configuration 71

© Virtual Access 2015

12.1 IPv4 routes 71
12.2 IPv6 routes 72
13 BGP (Border Gateway Protocol) 74
13.1 Configuring the BGP web interface 74
13.2 Optionally configure BGP route map 75
13.3 Configure BGP neighbours 76
13.4 Routes statistics 76
13.5 BGP UCI interface 77
14 Configuring WiFi 80
14.1 Configuring WiFi through the web interface 80
14.2 Configuring WiFi in AP mode on an existing Ethernet interface 80
14.3 Configuring WiFi in AP mode on a new interface 84
14.4 Configuring WiFi in client mode 89
14.5 Configuring WiFi via UCI 93
14.5.1 Configuring Wi-Fi in AP mode on an existing Ethernet interface 93
14.5.2 Configuring WiFI on a new interface 95
14.6 Configuring WiFi in client mode 97
15 Configuring a 3G/4G connection 99
16 Configuring SMS 102
16.1 Monitoring SMS 103
16.2 Outgoing messages 103
17 Configuring Multi-WAN 104
17.1 Multi-WAN web interface 104
17.2 Multi-WAN UCI interface 107
18 Automatic operator selection 110
18.1 Introduction to automatic operator selection 110
18.2 Configuring automatic operator selection 110
18.3 Configuring automatic operator selection via the web interface 110
18.3.1 PMP + roaming: pre-empt enabled 110
18.3.1.1 Creating primary predefined interface 111
18.3.1.2 Setting multi-WAN options for primary predefined interface 113
18.3.1.3 Setting options for automatically created interfaces 115
18.3.2 PMP + roaming: pre-empt disabled 120
18.3.3 Roaming: no PMP defined 121
18.3.4 Disable roaming 122
19 Configuring IPSec 123
19.1 Common settings 123
19.2 Connection settings 124
19.3 Shunt connection 128
19.4 Secret settings 128

20 Configuring firewall 131
20.1 Defaults section 131
20.2 Zones section 131
20.3 Forwarding sections 132
20.4 Redirects 133
20.5 Rules 134
20.6 Includes 135
20.7 IPv6 notes 135
20.8 Implications of DROP vs. REJECT 136
20.9 Note on connection tracking 137
20.10 Firewall examples 137
20.10.1 Opening ports 137
20.10.2 Forwarding ports (destination NAT/DNAT) 137
20.10.3 Source NAT (SNAT) 138
20.10.4 True destination port forwarding 139
20.10.5 Block access to a specific host 139
20.10.6 Block access to the internet using MAC 139
20.10.7 Block access to the internet for specific IP on certain times 139
20.10.8 Restricted forwarding rule 140
20.10.9 Transparent proxy rule (same host) 140
20.10.10 Transparent proxy rule (external) 140
20.10.11 Simple DMZ rule 141
20.10.12 IPSec passthrough 141
20.10.13 Manual iptables rules 142
20.11 Firewall management 142
20.12 Debug generated rule set 143
21 Configuring SNMP 144
21.1 agent 144
21.2 system 145
21.3 com2sec 145
21.4 access 148
21.5 SNMP traps 149
22 Configuring HTTP server 150
22.1 Server settings 150
22.2 HTTPS certificate settings and creation 152
22.3 Basic authentication (httpd.conf) 153
22.4 Securing uHTTPd 154
22.5 SSH server configuration 154
23 Configuring ADSL 155
23.1 What is ADSL technology? 155

23.2 ADSL connections 155
23.3 ADSL connection options on your router 155
23.4 Configuring ADSL PPP connection via the web interface 156
23.5 Configuring an ADSL PPPoA connection 157
23.6 Configuring an ADSL PPPoEoA connection 159
23.7 Configuring an ADSL bridge connection with static IP 162
23.8 Configuring ADSL via UCI 165
23.8.1 Configuring an ADSL PPPoA connection via UCI 165
23.8.2 Configuring an ADSL PPPoEoA connection via UCI 166
24 Virtual Router Redundancy Protocol (VRRP) 169
24.1 Software versions 169
24.2 VRRP web interface 170
24.3 Configuring VRRP using UCI 173
25 Dial modem 175
25.1 V.90 modem scenarios 175
25.2 Setting up the V.90 physical port connection 175
25.3 Configuring the modem as a dial out interface via UCI interface 176
25.4 Configuring the modem as a dial in interface via UCI 177
25.4.1 Mgetty settings 177
25.4.2 Dial in interface settings 178
25.4.3 Management user settings 179
26 ISDN pseudowire 180
26.1 Introduction 180
26.2 Pseudowire functionality 181
26.3 ISDN pseudowire in client role 181
26.3.1 Configuring LCR using UCI 181
26.3.2 Configuring Asterisk using UCI 182
26.4 ISDN pseudowire in client and provider role (back-to-back) 183
26.4.1 Configuring LCR using UCI 183
26.4.2 Configuring Asterisk using UCI 184
27 Analogue Leased Line interface 187
27.1 Terminal Server: V.23 modem emulation 187
27.2 CESoPSN: transparent mode 187
27.3 Gain and attenuation control 187
27.4 ALL interface 188
27.4.1 ALL status 188
27.4.2 ALL statistics 189
27.4.3 ALL wiring 189
28 Configuring CESoPSN 191
28.1 What is CESoPSN? 191

28.2 Configuring CESoPSN using UCIJK 191
28.2.1 Main settings 191
28.3 Port settings 192
28.3.1 ALL interface settings 194
28.3.2 Dual X.21 interface settings 194
29 Dynamic Multipoint Virtual Private Network (DMVPN) 195
29.1 The advantage of using DMVPN 195
29.2 DMVPN scenarios 195
29.3 Configuring DMVPN via the web interface 197
29.3.1 Configuring IPSec for DMVPN 198
29.4 DMVPN hub settings 204
29.5 UCI interface 205
29.5.1 IPSec configuration using CLI 205
29.6 Configuring DMVPN using CLI 207
30 Terminal Server 209
30.1 Introduction 209
30.2 Terminal Server interfaces 209
30.3 Configuring Terminal Server 209
30.3.1 Configuring Terminal Server using the web interface 209
30.3.1.1 Main settings 209
30.3.1.2 Port settings 210
30.3.1.3 Port settings: general section 210
30.3.1.4 Port settings: serial section 212
30.3.1.5 Port settings: network section 214
30.4 Configuring Terminal Server using UCI 216
30.5 Terminal Server operation 226
30.5.1 General 226
30.5.2 Starting Terminal Server 226
30.5.3 Checking the status of Terminal Server 226
30.5.4 Stopping Terminal Server 227
31 GRE interfaces 228
31.1 GRE web interface 228
31.2 GRE UCI interface 230
32 Multicasting using PIM and IGMP interfaces 232
32.1 Configuring PIM and IGMP via the web interface 232
32.2 PIM and IGMP UCI interface 234
33 Dynamic Multipoint Virtual Private Network (DMVPN) 237
33.1 The advantage of using DMVPN 237
33.2 DMVPN scenarios 237

© Virtual Access 2015

33.3 Configuring DMVPN via the web interface 239
33.3.1 Configuring IPSec for DMVPN 240
33.4 DMVPN hub settings 246
33.5 UCI interface 247
33.5.1 IPSec configuration using CLI 247
33.6 Configuring DMVPN using CLI 249
34 Event system 251
34.1 Implementation of the event system 251
34.2 Supported events 251
34.3 Supported targets 251
34.4 Supported connection testers 252
34.5 Configuring the event system via the web interface 252
34.6 Configuring the event system via UCI 252
34.6.1 Main section 252
34.6.2 Forwardings 253
34.6.3 Connection testers 253
34.6.3.1 Ping connection tester 254
34.6.3.2 Link connection tester 254
34.6.4 Supported targets 255
34.6.4.1 Syslog target 255
34.6.4.2 Email target 256
34.6.4.3 SNMP target 257
34.6.4.4 Exec target 257
34.6.5 Example and export 258
35 Configuring SLA reporting on Monitor 264
35.1 Introduction 264
35.2 Configuring SLA reporting 264
35.2.1 Configuring a content template 264
35.3 Adding an SLA report 267
35.4 Viewing an SLA report 269
35.5 Viewing automated SLA reports 270
35.6 Configuring router upload protocol 271
36 Configuring SLA for a router 272
36.1 Configuring SLA for a router via the web interface 272
36.2 Configuring SLA for a router via UCI interface 274
36.3 SLA statistics 275
37 Diagnostics 277
37.1 ADSL diagnostics 277
37.1.1 ADSL PPPoA connections 277

37.1.2 ADSL PPPoEoA connections 277
37.1.3 ADSL bridge connections 278
37.2 ALL diagnostics 279
37.3 Automatic operator selection diagnostics via the web interface 280
37.3.1 Checking the status of the Multi-WAN package 280
37.4 Automatic operator selection diagnostics via UCI 281
37.5 CESoPSN diagnostics 283
37.5.1 cesop show config 283
37.5.2 cesop show status 285
37.5.3 cesop show stats 285
37.5.4 cesop clear stats 286
37.6 DMVPN diagnostics 287
37.7 File system diagnostics 289
37.8 Firewall diagnostics 290
37.8.1 IP tables 293
37.8.2 Debug 293
37.9 GPS diagnostic commands 294
37.10 Interfaces diagnostics 294
37.10.1 Interfaces status 294
37.10.2 Route status 295
37.10.3 Mobile status 295
37.10.4 ADSL status 296
37.11 ISDN pseudowire diagnostics 297
37.11.1 Packages 297
37.11.2 Asterisk CLI diagnostics 298
37.11.3 ISDN LED status 299
37.12 IPSec diagnostics 299
37.13 Multi-WAN diagnostics 300
37.14 PAD diagnostics 301
37.14.1 Showing Log 301
37.14.2 Debugging guidelines 302
37.15 Terminal Server diagnostics 303
37.16 VRRP diagnostics 304
37.16.1 VRRP diagnostics web interface 304
37.16.2 VRRP diagnostics using the command line interface 304
37.17 Diagnostics for WiFi AP mode 305
37.18 Diagnostics for WiFi client mode 305

© Virtual Access 2015

1 Introduction

Based on the very latest ADSL2+, WiFi and 3G HSPA+ technology, Virtual Access GW600 Series routers address the needs of today's businesses for managed resilient broadband connectivity. Point of Sale (POS), retail branch office, security monitoring and other key business applications demand managed connectivity that is cost-effective, high performance and resilient to network outage or last mile circuit failure.

Designed for managed network providers, GW6600 Series routers provide secure WAN connectivity for internet and private networking environments over both ADSL2+ and 3G broadband paths and incorporate optional 802.11n WiFi connectivity.

1.1 Document scope

This document covers the following models in the GW6600 Series.

Model	ADSL2+	Eth	WiFi	3G/HSPA+	4G/LTE	CDMA 450	Dual SIM Socket	V92 Modem	Analogue Leased Line	ISDN BRI
GW6610	1	4						●	●	●
GW66110W	1	4	1					●	●	●
GW6630	1	4		✓			✓	●	●	●
GW6630W	1	4	1	✓			✓	●	●	●
GW6640	1	4		✓	✓		✓	●	●	●
GW6640W	1	4	1	✓	✓		✓	●	●	●
GW6650	1	4				✓		●	●	●
GW6650W	1	4	1			✓		●	●	●

Throughout this document we use the host name 'VA_router'.

© Virtual Access 2015

2 GW6600 Series hardware

2.1 Hardware specification

2.1.1 GW6600 Series router model variants

Model	ADSL2+	Eth	WiFi	3G/HSPA+	4G/LTE	CDMA 450	Dual SIM Socket	V92 Modem	Analogue Leased Line	ISDN BRI
GW6610	1	4						●	●	●
GW66110W	1	4	1					●	●	●
GW6630	1	4		✓			✓	●	●	●
GW6630W	1	4	1	✓			✓	●	●	●
GW6640	1	4		✓	✓		✓	●	●	●
GW6640W	1	4	1	✓	✓		✓	●	●	●
GW6650	1	4				✓		●	●	●
GW6650W	1	4	1			✓		●	●	●

2.2 Hardware features

- Dual SIM sockets
- Dual antenna SMA connectors
- Four 10/100 Mbps Ethernet ports
- Optional V.92, ALL or ISDN ports
- Optional WiFi
- Optional SIM cover

2.3 GSM technology

- HSPA+
- EDGE/GPRS
- Download up to 21Mbps
- Upload up to 5.76Mbps
- 2100/1900/900/850MHz bands
- LTE 2100/1900/1800/850/2600/900/800MHz bands

© Virtual Access 2015

2.4 Power supply

The GW6600 Series router has three power supply options:

- 100V-240V AC PSU (standard)
- 100V-240V AC PSU with extended temperature support -20°C to +70°C
- 10V-30V DC power lead

2.5 Dimensions

Unit size:	224W 158D 34H mm
Unit weight:	916g

2.6 Compliance

The GW6600 Series router is compliant and tested to the following standards:

Safety	EN60950-1: 2006 + A12: 2011
EMC	EN55022: 2010 Class B and EN55024: 2010
Environmental	ETSI 300 019-1-3 Sinusoidal Vibration and Shock ETSI 300 019-2-3 Random Vibration

2.7 Operating temperature range

The operating temperature range depends on the router's type of power supply.

Standard AC PSU:	0°C to +65°C
Optional industrial PSU	-20°C to +65°C
DC input cable	0°C to +65°C

2.8 Antenna

The GW6600 Series router has four SMA connectors for connection of up to four antennas for antenna diversity. Antenna diversity helps improve the quality of a wireless link by mitigating problems associated with multipath interference.

2.9 Components

To enable and configure connections on your router, it must be correctly installed.

The GW6600 Series router contains an internal web server that you use for configurations. Before you can access the internal web server and start the configuration, ensure the components are correctly connected and that your PC has the correct networking setup.

The GW6600 Series router comes with the following components as standard:

1 x GW6600 Series router (model interfaces vary)	
1 x Ethernet cable RJ45 to RJ45 (yellow).	
1 x ADSL cable: RJ11 to RJ11 (purple)	
1 x 12V power supply unit (2 part).	

Table 1: GW6600 Series router standard components

Optional components include:

1 x V.90 cable: RJ11 to RJ45 (blue) (IE/EU customers only)	
1 x V.90 cable: RJ11 to RJ45 BT cable (blue) (UK customers only)	
1 x ISDN cable: RJ45 to RJ45 (yellow)	
1 x lockable SIM cover.	
1 x 3G antenna	
1 x WiFi antenna	
Extra antennas	Virtual Access supplies a wide range of antennas for 3G and WiFi. Please visit our website: www.virtualaccess.com or contact Virtual Access for more information.

Table 2: GW6600 Series router optional components

2.10 Inserting the SIM cards

1. Ensure the unit is powered off.
2. Hold the SIM 1 card with the chip side facing down and the cut corner front left.

3. Gently push the SIM card into SIM slot 1 until it clicks in.
4. If using SIM 2 hold the SIM with the chip side facing down and the cut corner front left.
5. Gently push the SIM card into SIM slot 2 until it clicks in.

2.11 Connecting the SIM lock

Connect the SIM lock using the Allen key provided.

2.12 Connecting cables

Connect one end of the Ethernet cable into port A and the other end to your PC or switch.

2.13 Connecting the antenna

If only connecting one antenna, screw the antenna into the MAIN SMA connector.

If using more than one antenna, screw the main antenna into the MAIN SMA connector and the secondary antenna into the 3G-AUX SMA connector.

2.14 Connecting the WiFi antenna

If you are connecting one antenna, screw the antenna into either of the WiFi SMA connectors. You can use a second WiFi antenna if necessary.

2.15 Powering up

Plug the power cable into an electrical socket suitable for the power supply.

The GW6600 takes approximately 2 minutes to boot up. During this time, the power LED flashes.

Other LEDs display different diagnostic patterns during boot up.

Booting is complete when the power LED stops flashing and stays on steady.

2.16 Reset button

The reset button is used to request a system reset.

When you press the reset button all LEDs turn on simultaneously. The length of time you hold the reset button will determine its behaviour.

Press Duration	Behaviour
Less than 2 seconds	Normal reset.
Between 2 and 15 seconds	The router resets to factory configuration.

© Virtual Access 2015

Between 20 seconds and 30 seconds	Recovery mode.
Over 30 seconds	Normal reset.

3 GW6600 Series LED behaviour

3.1 Main LED behaviour

The GW6600 Series router has a single colour LED. When the router is powered on, the LED is green.

Figure 1: Example of power and config LED activity: power and config are on

The possible LED states are:

- Off
- Flashing slowing
- Flashing quickly
- On

The following table describes the possible LED behaviour and meanings.

Booting up		The GW6600 takes approximately 2 minutes to boot up. During this time, the power LED flashes. Other LEDs display different diagnostic patterns during boot up. Booting is complete when the power LED stops flashing and stays on steady
Power LED	On	Power
	Off	No power/boot loader does not exist.
Config LED	On	Unit running a valid configuration file.
	Flashing slowly	Unit running in recovery mode (2.5 flashes per second).
	Flashing quickly	Unit running in factory configuration (5 flashes per second).
ADSL SYN LED	On	Connected to DSLAM.
	Off	Not connected.
	Flashing	Connection negotiating.
ADSL DAT LED	On	Transmit data.
	Off	No data transmit.
SIM LEDs	On	SIM selected and registered on the network.
	Off	Not selected or SIM not inserted.
	Flashing	SIM selected and not registered on the network.

© Virtual Access 2015

Signal LEDs	None	PPP not connected or signal strength <= -113dBm.
	1	PPP connected and signal strength <= -89dBm.
	2	PPP connected and signal strength between -89dBm and -69dBm.
	3	PPP connected and signal strength >-69dBm.
V.92 SYN LED		
Applies to the following models: GW6631 GW6641	Off	Not connected.
	On	Connection established.
	Flashing	Modem training.
V.92 DAT LED		
Applies to the following models: GW6631 GW6641	Off	No data transmit.
	Flashing	Transmit data.
ALL SYN LED		
Applies to the following models: GW6610-ALL	On	CESOP enabled.
	Off	CESOP disabled.
ALL DAT LED		
Applies to the following models: GW6610-ALL	On	Receive data.
	Off	No data received.
ISDN top LED		
Applies to the following models: GW6610-ISDN	On	Audio channel active (dial tone or call in progress).
	Off	Audio channel inactive.
ISDN bottom LED		
Applies to the following models: GW6610-ISDN	On	Audio channel active (dial tone or call in progress).
	Off	BRI channel 2 inactive. Audio channel inactive.

Table 3: LED behaviour and descriptions

Note: When PPP is not connected, none of the signal LEDs will light regardless of signal strength.

© Virtual Access 2015

3.2 Ethernet port LED behaviour

The Ethernet port has two LEDs: a LINK LED (green) and an ACT LED (amber). When looking at the port, the LED on the left hand side is the LINK LED, and the ACT LED is on the right hand side.

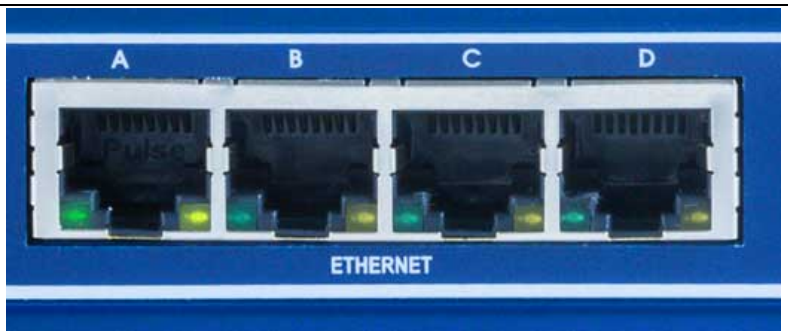


Figure 2: Ethernet LED activity

Link LED (green)	Off	No physical Ethernet link detected.
	On	Physical Ethernet link detected.
ACT LED (amber)	Off	No data is being transmitted/received over the link.
	Flashing	Data is being transmitted/received over the link.
Note: LED descriptions apply to all GW6600 Series models.		

4 Factory configuration extraction from SIM card

Virtual Access routers have a feature to update the factory configuration from a SIM card. This allows you to change the factory configuration of a router when installing the SIM.

1. Make sure the SIM card you are inserting has the required configuration written on it.
2. Ensure the router is powered off.
3. Hold the SIM 1 card with the chip side facing down and the cut corner front left.
4. Gently push the SIM card into SIM slot 1 until it clicks in.
5. Power up the router.

Depending on the model, the power LED and/or the configuration LED flash as usual.

The SIM LED starts flashing. This indicates the application responsible for 3G and configuration extraction management is running. It also means the update of the configuration is happening.

When the update is finished, depending on the model, the power LED and/or the configuration LED blink alternatively and very fast for 20 seconds.

5 Accessing the router

Access the router using either Ethernet or the 3G/4G interface.

5.1 Over Ethernet

The CLI can also be accessed over Ethernet, by default using Secure Shell (SSH) and optionally over Telnet

To access CLI over Ethernet start an SSH client and connect to the router's management IP address, on port 22: **192.168.100.1/24**. Then enter the default username and password.

Username: **Root**

Password: **Admin**

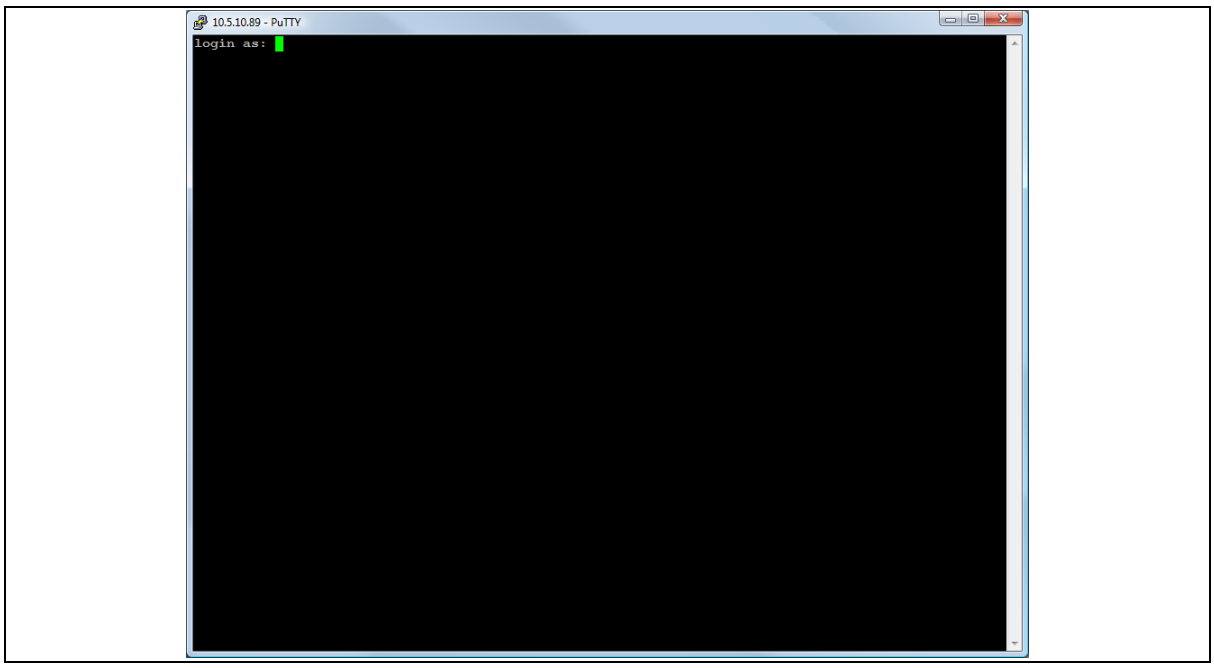


Figure 3: SSH CLI logon screen

5.2 Over a 3G or 4G interface

You can also access the CLI over the router's 3G or 4G interface using Secure Shell (SSH) and optionally over Telnet.

To access CLI start an SSH client and connect to the router's 3G or 4G IP interface on port 22: **192.168.100.1/24**. Then enter the default username and password.

Username: **Root**

Password: **Admin**

6 Upgrading router firmware

6.1 Upgrading firmware using the web interface

Copy the new firmware issued by Virtual Access to a PC connected to the router.

In the top menu, select **System tab > Backup/Flash Firmware**.

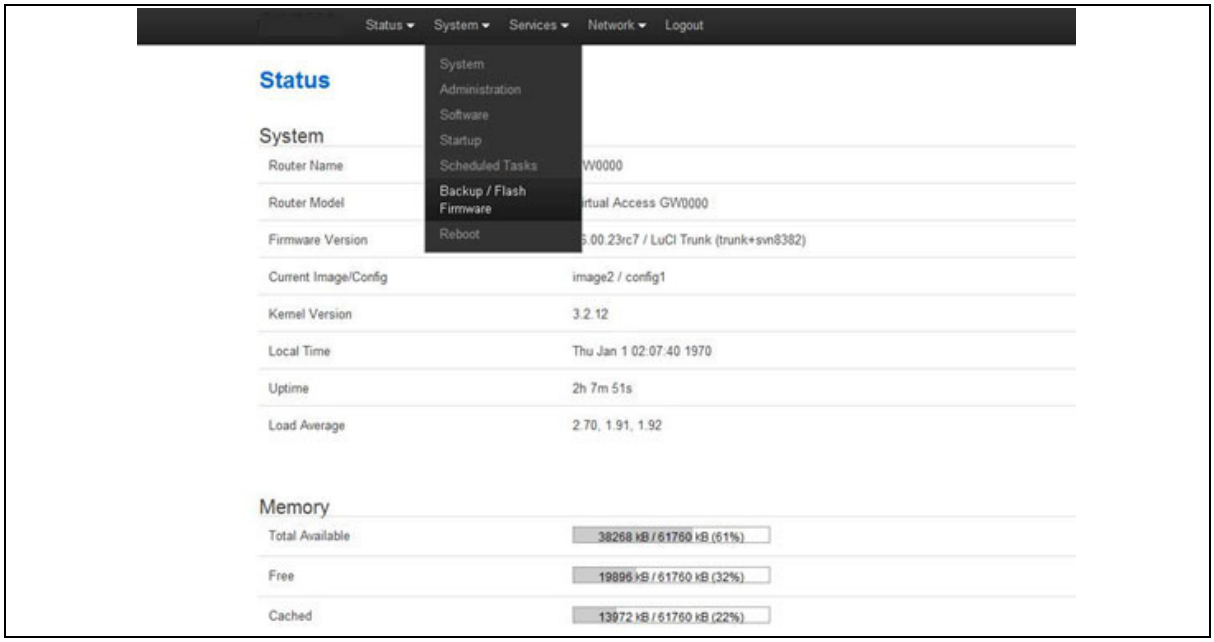


Figure 4: The system menu

The Flash operations page appears.

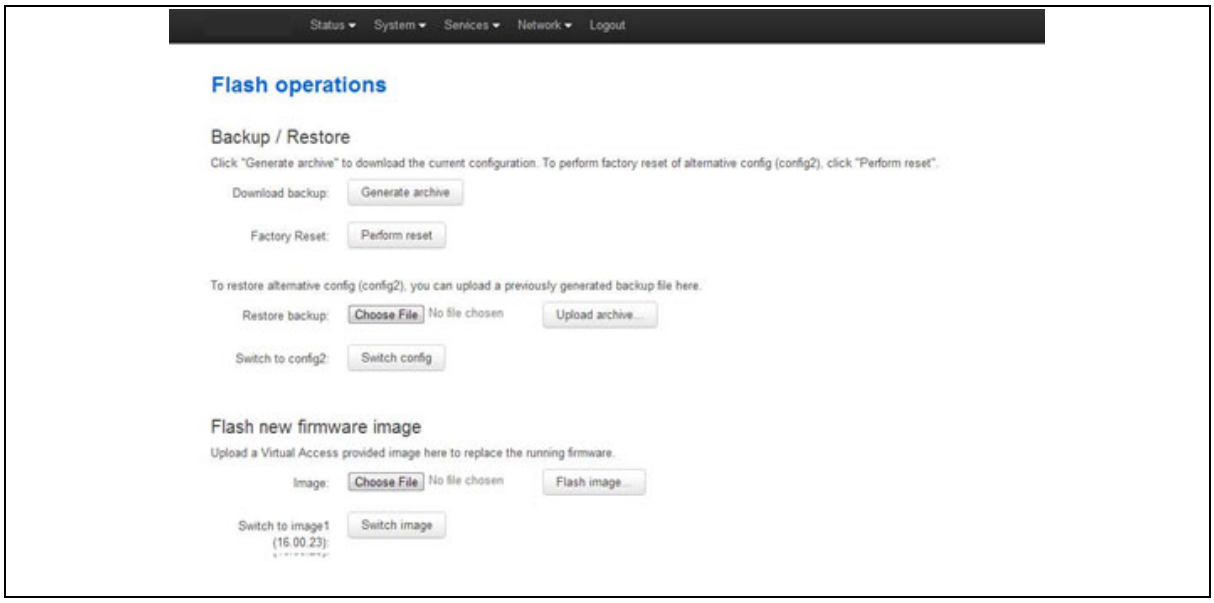


Figure 5: The flash operations page

Under Flash new firmware image, click **Choose File** or **Browse**.

Note: the button will vary depending on the browser you are using.

Select the appropriate image and then click **Flash Image**. The Flash Firmware – Verify page appears.

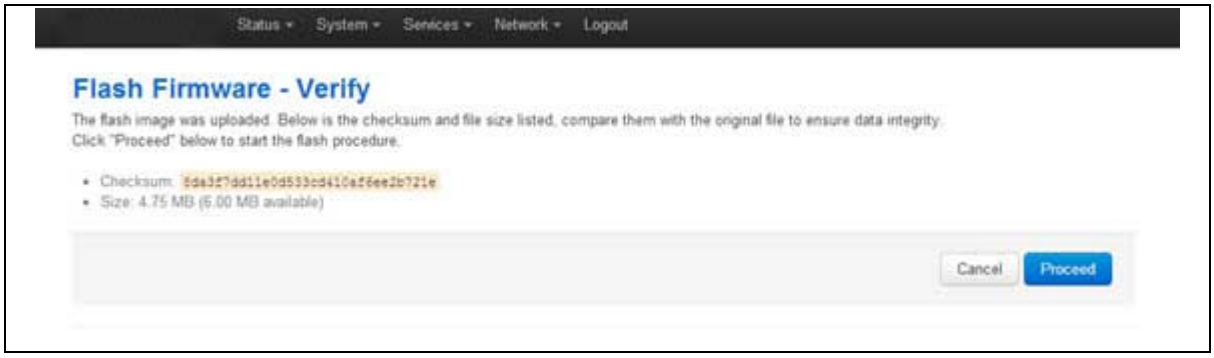

Status
System
Services
Network
Logout
Flash Firmware - Verify
The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity.
Click "Proceed" below to start the flash procedure.
Checksum: 8da3f7dd11e0d533cd410af6ee2b721e
Size: 4.75 MB (6.00 MB available)
Cancel
Proceed

Figure 6: The flash firmware - verify page

Click **Proceed**. The System – Flashing… page appears.

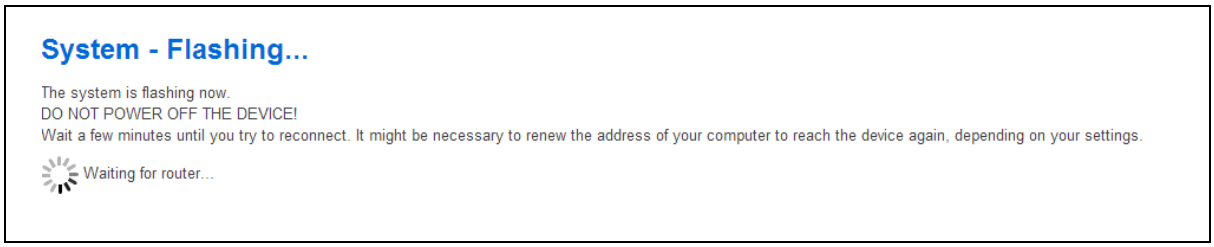

System - Flashing...
The system is flashing now.
DO NOT POWER OFF THE DEVICE!
Wait a few minutes until you try to reconnect. It might be necessary to renew the address of your computer to reach the device again, depending on your settings.
Waiting for router...

Figure 7: The system – flashing…page

When the 'waiting for router' icon disappears, the upgrade is complete, and the login homepage appears.

To verify that the router has been upgraded successfully, click **Status** in the top menu. The Firmware Version shows in the system list.

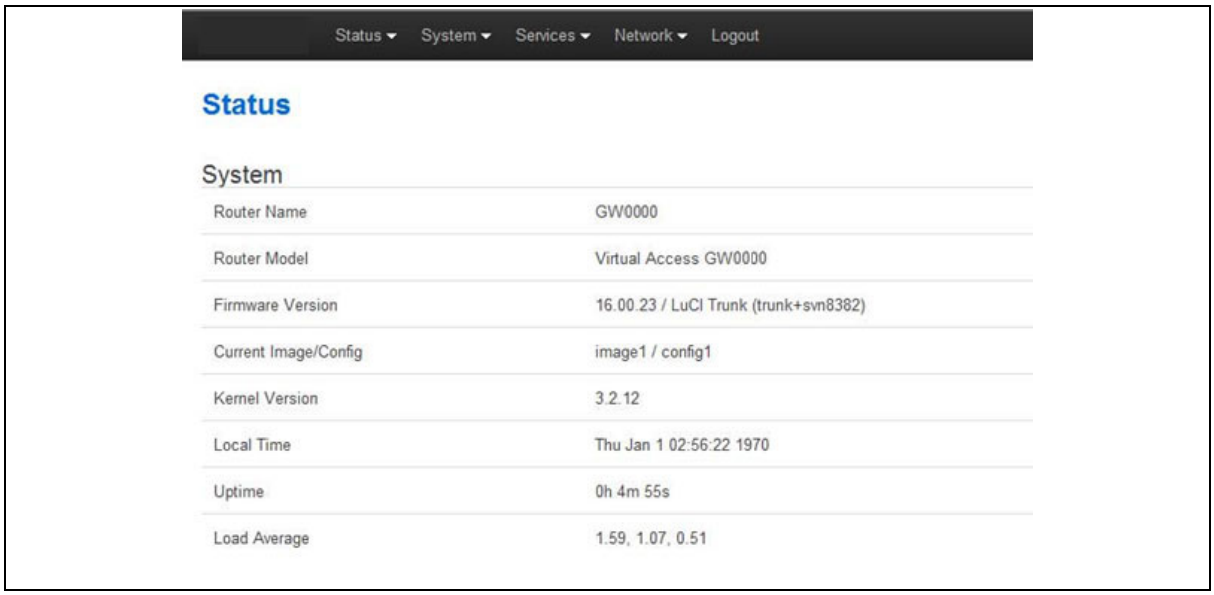


Figure 8: The status page

6.2 Upgrading firmware using CLI

To upgrade firmware using CLI, you will need a TFTP server on a connected PC.

Open up an SSH or Telnet session to the router.

Enter in the relevant **username** and **password**.

To change into the temp folder, enter:

cd /tmp

To connect to your TFTP server, enter:

```
atftp x.x.x.x
```

(where x.x.x.x is the IP of your PC).

Press **Enter**.

While in the TFTP application, to get the image, enter:

```
get GIG-15.00.38.image
```

Note: this is an example, substitute the correct file name.

When the image has downloaded, to leave TFPT and get back into the command line, enter:

```
quit
```

To write the image into the alternative image, enter:

```
mtd write GIG-15.00.38.image altimage
```

Note: this is an example, substitute the correct file name.

To set the next image to boot to the alternative image, enter:

```
vacmd set next image altimage.
```

For your configuration changes to apply, you must reboot your router. Enter:

```
reboot
```

7 File system

7.1 Configurations

Configurations are stored in folders at:

/etc/conf/factconf,

/etc/conf/config1

and

/etc/conf/config2

Multiple configuration files exist in each folder. Each file contains configuration parameters for different areas of functionality in the system.

A symbolic link exists at:

/etc/conf/config, which always points to one of factconf, config1 or config2.

Files that appear to be in **/etc/conf/config** are actually in **/etc/conf/factconf|config1|config2** depending on which configuration is active.

If **/etc/conf** is missing on start-up, for example on first boot, the links and directories are created with configuration files copied from **/overlay/etc/config/**.

At any given time, only one of the configurations is the active configuration.

To show the active configuration file, enter:

```
root@VA_router:~# vacmd show current config
```

To set the boot configuration to run on next reboot, enter:

```
root@VA_router:~# vacmd set next config [factconf|config1|config2]
```

7.1.1 High level configuration commands

To show the configuration currently running, enter:

```
root@VA_router:~# vacmd show current config
```

To show the configuration to run after the next reboot, enter:

```
root@VA_router:~# vacmd show next config
```

To set the configuration to run after the next reboot, enter:

```
root@VA_router:~# vacmd set next config [factconf|config1|config2]
```

Image files

The system allows for two firmware image files named image1 and image2.

One is the current image that is running and the other is the alternate image.

7.1.2 Configuration file syntax

The configuration files consist of sections that contain one or more config statements. These optional statements define the actual values.

Below is an example of a simple configuration file.

```
package 'example'
config 'example' 'test'
        option   'string'      'some value'
        option   'boolean'     '1'
        list     'collection'  'first item'
        list     'collection'  'second item'
```

The config `'example' 'test'` statement defines the start of a section with the type example and the name test. There can also be so called anonymous sections with only a type, but no name identifier. The type is important so the processing programs can decide how to treat the enclosed options.

The option `'string' 'some value'` and option `'boolean' '1'` lines define simple values within the section.

Note: there are no syntactical differences between text and boolean options. Boolean options may have one of the values `'0', 'no', 'off'` or `'false'` to specify a false value or `'1', 'yes', 'on'` or `'true'` to specify a true value.

In the lines starting with a list keyword, an option with multiple values is defined. All list statements that share the same name, collection in this example, will be combined into a single list of values with the same order as in the configuration file.

The indentation of the option and list statements is a convention to improve the readability of the configuration file but it is not syntactically required.

Usually, you do not need to enclose identifiers or values in quotes. Quotes are only required if the enclosed value contains spaces or tabs. Also, it is legal to use double instead of single quotes when typing configuration options.

All of the examples below are valid syntax:

```
option example value
```

```
option 'example' value
```

```
option example “value”
option “example”    'value'
option   'example' “value”
```

In contrast, the following examples are not valid syntax:

option ‘example’ value Missing quotes around the value.

option 'example” “value' Quotes are unbalanced.

It is important to know that identifiers and config file names may only contain the characters a-z, 0-9 and _. Option values may contain any character, as long they are properly quoted.

7.1.3 Command line utility

For configuration, the system emulates a subset of the Unified Configuration Interface (UCI). This section describes the usage guide for the UCI command line.

When there are multiple rules next to each other, UCI uses array-like references for them. If there are 8 NTP servers, UCI will let you reference their sections as timeserver.@timeserver[0] for the first rule or timeserver.@timeserver[7] for the last one.

```
root@VA_router:~# uci
Usage: uci [<options>] <command> [<arguments>]
Commands:
        batch
        list
        export     [<config>]
        import     [<config>]
        changes    [<config>]
        commit     [<config>]
        add        <config> <section-type>
        add_list   <config>.<section>.<option>=<string>
        show       [<config>[.<section>[.<option>]]]
        get        <config>.<section>[.<option>]
        set        <config>.<section>[.<option>]=<value>
        delete     <config>[.<section[.<option>]]
        rename     <config>.<section>[.<option>]=<name>
        revert     <config>[.<section>[.<option>]]
        reorder    <config>.<section>=<position>
```

```
Options:
        -c <path>  set the search path for config files (default:
/etc/config)
        -d <str>   set the delimiter for list values in uci show
        -f <file>  use <file> as input instead of stdin
        -L         do not load any plugins
        -m         when importing, merge data into an existing package
        -n         name unnamed sections on export (default)
        -N         don't name unnamed sections
        -p <path>  add a search path for config change files
        -P <path>  add a search path for config change files and use as
default
        -q         quiet mode (don't print error messages)
        -s         force strict mode (stop on parser errors, default)
        -S         disable strict mode
        -X         do not use extended syntax on 'show'
```

Command	Target	Description
export	[<config>]	Exports the configuration in a machine readable format. It is used internally to evaluate configuration files as shell scripts.
import	[<config>]	Imports configuration files in UCI syntax.
add	<config> <section-type>	Adds an anonymous section of type-section type to the given configuration.
add_list	<config>.<section>.<option>=<string>	Adds the given string to an existing list option.
show	[<config>[.<section>[.<option>]]]	Shows the given option, section or configuration in compressed notation.
get	<config>.<section>[.<option>]	Gets the value of the given option or the type of the given section.
Set	<config>.<section>[.<option>]=<value>	Sets the value of the given option, or adds a new section with the type set to the given value.
delete	<config>[.<section[.<option>]]	Deletes the given section or option.

Table 1: Commands, target and their descriptions

Note: all operations do not act directly on the configuration files. A commit command is required after you have finished your configuration.

```
root@VA_router:~# uci commit
```

7.1.3.1 Command line utility examples

To export an entire configuration, enter:

```
root@VA_router:~# uci export
```

To export the configuration for a single package, enter: `uci export <package>`.

```
root@VA_router:~# uci export system
package system

config system 'main'
        option hostname 'VA_router'
        option zonename 'Europe/Dublin'
        option timezone 'GMT0IST,M3.5.0/1,M10.5.0'
        option cronloglevel '9'
        option log_ip '0.0.0.0'
        option log_port '514'

config timeserver 'ntp'
        list server '0.openwrt.pool.ntp.org'
        list server '1.openwrt.pool.ntp.org'
        list server '2.openwrt.pool.ntp.org'
        list server '3.openwrt.pool.ntp.org'
```

To show an alternate view of a configuration file, enter `uci show`:

```
root@VA_router:~# uci show system
system.main=system
system.main.hostname=VA_router
system.main.zonename=Europe/Dublin
system.main.timezone=GMT0IST,M3.5.0/1,M10.5.0
system.main.cronloglevel=9
system.main.log_ip=0.0.0.0
system.main.log_port=514
system.ntp=timeserver
system.ntp.server=0.openwrt.pool.ntp.org 1.openwrt.pool.ntp.org
2.openwrt.pool.ntp.org 3.openwrt.pool.ntp.org
```

© Virtual Access 2015

To display just the value of an option, enter:

```
root@VA_router:~# uci get system.main.hostname
VA_router
```

7.1.4 Configuration copying and deleting

Manage configurations using directory manipulation.

To remove the contents of the current folder, enter:

```
root@VA_router:/etc/config1# rm –f *
```

To remove the contents of a specific folder regardless of the current folder (config2), enter:

```
root@VA_router:/ # rm –f /etc/config1/*
```

To copy the contents of one folder into another (config2 into config1), enter:

```
root@VA_router:/etc/config1# cp /etc/config2/* /etc/config1
```

7.1.5 Image files

The system allows for two firmware image files:

- image1, and
- image2

Two firmware images are supported to enable the system to rollback to a previous firmware version if the upgrade of one fails.

The image names (image1, image2) themselves are symbols that point to different partitions in the overall file system. A special image name “altimage” exists which always points to the image that is not running.

The firmware upgrade system always downloads firmware to “altimage”.

7.1.6 Viewing files

To view a text or configuration file in the system, enter the cat command:

```
root@VA_router:~# cat /etc/config/dropbear
config dropbear
        option PasswordAuth 'on'
        option BannerFile '/etc/banner'
        option RootPasswordAuth 'yes'
        option IdleTimeout '1800'
        option Port '22'
```

To view files in the current folder, enter `ls`:

```
root@VA_router:/# ls
bin      etc      lib      opt      sbin     usr
bkrepos  home     linuxrc  proc     sys      var
dev      init     mnt      root     tmp      www
```

Other common Linux commands are available such as: `top, grep, tail, head, more, less`.

Typical pipe and redirect operators are available: `>, >>, <, |`

7.1.7 Copying files

To change current folder, enter `cd`:

```
root@VA_router:~# cd /etc/config1
root@VA_router:/etc/config1#
```

Note: if the specified directory is actually a link to a directory, the real directory will be shown in the prompt.

To remove the contents of the current folder, use:

```
root@VA_router:/etc/config1# rm –f *
```

Warning: the above command makes irreversible changes.

To remove the contents of a specific folder regardless of the current folder, use:

```
root@VA_router:~#  rm –f /etc/config1/*
```

To copy the contents of one folder into another, for example config2 into config1, use:

```
root@VA_router:~# cp /etc/config2/* /etc/config1/*
```

7.1.8 Editing files

The config can be edited using uci commands or via the web GUI.

7.1.9 Processes and jobs

To view scheduled jobs, enter:

```
root@VA_router:~# crontab -l
```

Note: currently there are no scheduled jobs.

To view running processes, enter:

```
root@VA_router:~# ps
  PID USER       VSZ STAT COMMAND
    1 root      1536 S    init
    2 root         0 SW   [kthreadd]
    3 root         0 SW   [ksoftirqd/0]
    4 root         0 SW   [kworker/0:0]
    5 root         0 SW   [kworker/u:0]
    6 root         0 SW<  [khelper]
... 1796 root      1540 S    /usr/bin/ifplugd -i eth0 -I -l -x lan2
 1879 root      7352 S    /sbin/dsl_cpe_control -i -n /sbin/dsl_notify.sh -
a /tmp/dsl.scr
 2017 root      1540 S    /usr/bin/ifplugd -i eth1 -I -l -x lan
 2178 root      1540 S    /usr/bin/ifplugd -i eth2 -I -l -x lan3
 2297 root      2256 S    {va_hdl.lua} /usr/bin/lua /usr/sbin/va_hdl.lua
$.ip ip
```

To kill a process, enter the PID:

```
root@VA_router:~# kill 2297
```

7.1.10 System information

General information about software and configuration used by the router is displayed just after login or is available if you enter the following commands.

```
root@VA__router:~# vacmd show vars
VA_SERIAL:              00E0C8121215
 VA_MODEL:               GW6610-ALL
 VA_ACTIVEIMAGE:         image2
 VA_ACTIVECONFIG:        config1
 VA_IMAGE1VER:           VIE-16.00.44
 VA_IMAGE2VER:           VIE-16.00.44
VA_BLDREV:              91a7f87ed61ca919e78f1c8e3cb840264f4887bb
 VA_REGION:              EU
 VA_WEBVER:              00.00.00

VA_HWREV:               a
 VA_TOPVER:              16.00.44
```

Shows the general software and configuration details of the router.

8 Command Line Interface

8.1 Basics

The system has an SSH server typically running on port 22.

The system provides a Unix command line. Common Unix commands are available such as ls, cd, cat, top, grep, tail, head, more. Typical pipe and redirect operators are available: >, >>, <, |

For configuration, the system uses the “Unified Configuration Interface” (UCI). See the next section for more detail.

The factconf default password for the root user is ‘admin’.

To change the factconf default password, enter:

```
root@VA_router:/# passwd
Current Password: ******
New Password: **********
Confirm New Password: **********
```

To reboot the system, enter:

```
root@VA_router:/# reboot
The system log can be viewed as follows:
root@VA_router:/# logread

root@VA_router:/# logread | tail

root@VA_router:/# logread | more

root@VA_router:/# logread –f
```

These commands will show the full log, end of the log, paged log and continuously. Use Ctrl-C to stop the continuous output.

To view a text or configuration file in the system, enter:

```
root@VA_router:/# cat /etc/ppp/options

logfile /dev/null
nocrtscts
lock
debug
refuse-chap
kdebug 7
record /tmp/ppp.log
```

To view files in the current folder, enter:

```
root@VA_router:/# ls -1

drwxrwxr-x    2 root     root   642 Jul 16  2012 bin
drwxr-xr-x    5 root     root  1020 Jul  4 01:27 dev
drwxrwxr-x    1 root     root     0 Jul  3 18:41 etc
drwxr-xr-x    1 root     root     0 Jul  9  2012 lib
drwxr-xr-x    2 root     root     3 Jul 16  2012 mnt
drwxr-xr-x    7 root     root     0 Jan  1  1970 overlay
dr-xr-xr-x   58 root     root     0 Jan  1  1970 proc
drwxr-xr-x   16 root     root   223 Jul 16  2012 rom
drwxr-xr-x    1 root     root     0 Jul  3 22:53 root
drwxrwxr-x    2 root     root   612 Jul 16  2012 sbin
drwxr-xr-x   11 root     root     0 Jan  1  1970 sys
drwxrwxrwt   10 root     root   300 Jul  4 01:27 tmp
drwxr-xr-x    1 root     root     0 Jul  3 11:37 usr
lrwxrwxrwx    1 root     root     4 Jul 16  2012 var -> /tmp
drwxr-xr-x    4 root     root    67 Jul 16  2012 www
```

To change current folder, enter:

```
root@VA_router:/# cd /etc/ppp
root@VA_router:/etc/ppp#
To view scheduled jobs:
root@VA_router:/# crontab –l
```

To view currently running processes:

```
root@VA_router:/# ps
 PID  Uid     VmSize Stat Command
    1 root        356 S   init
    2 root            DW  [keventd]
    3 root            RWN [ksoftirqd_CPU0]
    4 root            SW  [kswapd]
    5 root            SW  [bdflush]
    6 root            SW  [kupdated]
    8 root            SW  [mtdblockd]
   89 root        344 S   logger -s -p 6 -t
   92 root        356 S   init
   93 root        348 S   syslogd -C 16
   94 root        300 S   klogd
  424 root        320 S   wifi up
549 root        364 S   httpd -p 80 -h /www -r VA_router
  563 root        336 S   crond -c /etc/crontabs
6712 root        392 S   /usr/sbin/dropbear
6824 root        588 S   /usr/sbin/dropbear
7296 root        444 S   -ash
  374 root        344 R   ps ax
  375 root        400 S   /bin/sh /sbin/hotplug button
  384 root        396 R   /bin/sh /sbin/hotplug button
  385 root            RW  [keventd]
```

8.2 Unified Configuration Interface (UCI)

The system uses Unified Configuration Interface (UCI) for central configuration management. All the most common and useful configuration settings can be accessed and configured using the uci system.

UCI consists of a command line utility 'uci', the files containing the actual configuration data, and scripts that take the configuration data and apply it to the proper parts of the system, such as the networking interfaces, or the web server.

The uci command is the preferred way of managing the configuration. Currently, you can directly access files, but this is not guaranteed for the future.

A simple example of using the uci utility is shown below.

```
root@VA_router:/# uci show network
network.loopback=interface
network.loopback.ifname=lo
network.loopback.proto=static
network.loopback.ipaddr=127.0.0.1
network.loopback.netmask=255.0.0.0
network.lan=interface
network.lan.ifname=eth0
network.lan.proto=dhcp
network.wan=interface
network.wan.username=foo
network.wan.password=bar
network.wan.proto=3g
network.wan.device=/dev/ttyACM0
network.wan.service=umts
network.wan.auto=0
network.wan.apn=arkessa.com
network.@va_switch[0]=va_switch
network.@va_switch[0].eth0=A B C
network.@va_switch[0].eth1=D
root@VA_router:/# uci set network.wan.apn=hs.vodafone.ie
root@VA_router:/# uci commit
root@VA_router:/# uci show network.wan
network.wan=interface
network.wan.username=foo
network.wan.password=bar
network.wan.proto=3g
network.wan.device=/dev/ttyACM0
network.wan.service=umts
network.wan.auto=0
network.wan.apn=hs.vodafone.ie
root@VA_router:/#
```

Below is a guide for the UCI command line and some further examples of how to use this powerful utility.

When there are multiple rules next to each other, UCI uses array-like references for them. If there are 8 NTP servers, UCI will let you reference their sections as

timeserver.@timeserver[0] for the first or timeserver.@timeserver[7] for the last one.

You can also use negative indexes, such as timeserver.@timeserver[-1]. "-1" means "the last one, and "-2" means the second-to-last one. This is useful when appending new rules to the end of a list. See examples below.

```
root@VA_router:/lib/config# uci

Usage: uci [<options>] <command> [<arguments>]

Commands:
      export     [<config>]
      import     [<config>]
      changes    [<config>]
      commit     [<config>]
      add        <config> <section-type>
      add_list   <config>.<section>.<option>=<string>
      show       [<config>[.<section>[.<option>]]]
      get        <config>.<section>[.<option>]
      set        <config>.<section>[.<option>]=<value>
      delete     <config>[.<section[.<option>]]
      rename     <config>.<section>[.<option>]=<name>
      revert     <config>[.<section>[.<option>]]
Options:
      -c <path>  set the search path for config files (default:
/etc/config)
      -d <str>   set the delimiter for list values in uci show
      -f <file>  use <file> as input instead of stdin
      -m         when importing, merge data into an existing package
      -n         name unnamed sections on export (default)
      -N         don't name unnamed sections
      -p <path>  add a search path for config change files
      -P <path>  add a search path for config change files and use as
default
      -q         quiet mode (don't print error messages)
      -s         force strict mode (stop on parser errors, default)
```

© Virtual Access 2015

```
      -S          disable strict mode
      -X          do not use extended syntax on 'show'
```

Command	Target	Description
commit	[<config>]	Writes changes of the given configuration file, or if none is given, all configuration files, to the filesystem. All "uci set", "uci add", "uci rename" and "uci delete" commands are staged into a temporary location and written to flash at once with "uci commit". This is not needed after editing configuration files with a text editor, but for scripts, GUIs and other programs working directly with UCI files.
export	[<config>]	Exports the configuration in a machine readable format. It is used internally to evaluate configuration files as shell scripts.
import	[<config>]	Imports configuration files in UCI syntax.
changes	[<config>]	Lists staged changes to the given configuration file or if none given, all configuration files.
Add	<config> <section-type>	Adds an anonymous section of type section-type to the given configuration.
add_list	<config>.<section>.<option>=<string>	Adds the given string to an existing list option.
show	[<config>[.<section>[.<option>]]]	Shows the given option, section or configuration in compressed notation.
get	<config>.<section>[.<option>]	Gets the value of the given option or the type of the given section.
Set	<config>.<section>[.<option>]=<value>	Sets the value of the given option, or add a new section with the type set to the given value.
delete	<config>[.<section[.<option>]]	Deletes the given section or option.
rename	<config>.<section>[.<option>]=<name>	Renames the given option or section to the given name.
revert	<config>[.<section>[.<option>]]	Reverts the given option, section or configuration file.

8.3 Configuration files

File	Description
Management	
/etc/config/autoload	Boot up Activation behaviour (typically used in factconf)
/etc/config/httpclient	Activator addresses and urls
/etc/config/monitor	Monitor details
Basic	
/etc/config/dropbear	SSH server options
/etc/config/dhcp	Dnsmasq configuration and DHCP settings
/etc/config/firewall	NAT, packet filter, port forwarding, etc.
/etc/config/network	Switch, interface, L2TP and route configuration
/etc/config/system	Misc. system settings including syslog
Other	
/etc/config/snmpd	SNMPd settings
/etc/config/uhttpd	Web server options (uHTTPd)
/etc/config/strongswan	IPSec settings

8.4 Configuration file syntax

The configuration files usually consist of one or more config statements, so called sections with one or more option statements defining the actual values.

Below is an example of a simple configuration file:

```
package 'example'
config 'example' 'test'
        option   'string'      'some value'
        option   'boolean'     '1'
        list     'collection'  'first item'
        list     'collection'  'second item'
```

The `config 'example' 'test'` statement defines the start of a section with the type example and the name test. There can also be so called anonymous sections with only a type, but no name identifier. The type is important for the processing programs to decide how to treat the enclosed options.

The option 'string' 'some value' and option 'boolean' '1' lines define simple values within the section. Note that there are no syntactical differences between text- and boolean options. Per convention, boolean options may have one of the values '0', 'no', 'off' or 'false' to specify a false value or '1' , 'yes', 'on' or 'true' to specify a true value.

In the lines starting with a list keyword, an option with multiple values is defined. All list statements that share the same name, collection in our example,

will be combined into a single list of values with the same order as in the configuration file.

The indentation of the option and list statements is a convention to improve the readability of the configuration file but it is not syntactically required.

Usually you do not need to enclose identifiers or values in quotes. Quotes are only required if the enclosed value contains spaces or tabs. Also it's legal to use double- instead of single-quotes when typing configuration options.

All of the examples below are valid syntax.

```
option example value
option 'example' value
option example "value"
option "example"    'value'
option   'example' "value"
```

In contrast, the following examples are not valid syntax.

```
option 'example" "value'
```

(quotes are unbalanced)

```
option example some value with space
```

(note the missing quotes around the value).

It is important to know that identifiers and config file names may only contain the characters a-z, 0-9 and _. Option values may contain any character, as long they are properly quoted.

8.5 Examples

No need to reboot.

After changing the port, uhttpd listens on from 80 to 8080 in the file /etc/config/uhttpd, save it. Then enter:

```
root@VA_router:~# uci commit uhttpd
```

then enter:

```
root@VA_router:~# /etc/init.d/uhttpd restart
```

Done. No reboot needed.

8.5.1 Export an entire configuration

```
root@VA_router:~# uci export httpd
package 'httpd'

config 'httpd'
      option 'port' '80'
      option 'home' '/www'

root@VA_router:~#
```

To show the configuration ‘tree’ for a given config, enter:

```
root@VA_router:~# uci show httpd
httpd.@httpd[0]=httpd
httpd.@httpd[0].port=80
httpd.@httpd[0].home=/www
root@VA_router:~#
```

8.5.2 Display just the value of an option

```
root@VA_router:~# uci get httpd.@httpd[0].port
80
root@VA_router:~#
High level image commands
The image running at present can be shown using the command:
root@VA_router:~# vacmd show current image
The image to run on next reboot can be set using the command:
root@VA_router:~# vacmd set next image [image1|image2|altimage]
root@VA_router:~# reboot
```

To retrieve new firmware from Activator, enter:

```
root@VA_router:~# vacmd hdl $$.img altimage
root@VA_router:~# vacmd set next image altimage
root@VA_router:~# reboot
```

9 Management configuration settings

This section details the configuration sections and parameters which are required to manage and monitor the device using Activator and Monitor.

Activator is a Virtual Access proprietary provisioning system, where specific router configurations and firmware can be stored.

Monitor is a Virtual Access proprietary tool, based on SNMP protocol, to monitor wide networks of deployed routers.

9.1 Autoload - boot up activation

This section contains the settings that specify how the device should behave with respect to Activation when it boots up. You can change the settings either directly in the configuration file or via appropriate uci set commands.

The autoload core section configures the basic functionality of the module which orchestrates the Activation process. It contains these settings:

Name	Type	Required	Default	Description
Enabled	boolean	yes	no	Enables autoload. Set to yes to activate at system boot.
StartTimer	integer	yes	10	Defines how long to wait after the boot up completes before starting activation.
RetryTimer	integer	yes	30	Defines how many seconds to wait between retries if a download of a particular autoload entry (see next table) fails.
NumberOfRetries	integer	yes	5	Defines how many retries to attempt before failing the overall activation sequence, backing off and trying the whole activation sequence again.
BackoffTimer	integer	yes	15	Defines how many minutes to back off for if a download and all retries fail. After the backoff period, the entire autoload sequence will start again.
BootUsingConfig	string	yes	altconfig	Specifies which configuration to boot up with after the activation sequence completes successfully.
BootUsingImage	string	yes	altimage	Specifies which image to boot up with after the activation sequence completes successfully.

The Autoload entry sections specify which files, and in which order they are downloaded when the autoload sequence executes.

Name	Type	Required	Default	Description
Configured	boolean	yes	no	Set to yes to make the autoload sequence process this entry.
SegmentName	string	yes	(none)	Where the downloaded file should be stored (config1 | config2 | altconfig | image1 | image2 | altimage). Typically only altconfig and altimage are used.
				$$.ini – request configuration
				$$.img – request firmware
RemoteFilename	string	yes	(none)	$$.vas – notify activator sequence is complete. $$.vas should always be requested last.

A sample autoload configuration is show below.

Note: as some values are exceptional (like $) they need to be appropriately escaped using uci set and show commands. This removes the need to know the correct escape sequences.

```
root@VA_router:/# uci show autoload
autoload.main=core
autoload.main.Enabled=yes
autoload.main.StartTimer=10
autoload.main.RetryTimer=30
autoload.main.NumberOfRetries=5
autoload.main.BackoffTimer=15
autoload.main.BootUsingConfig=altconfig
autoload.main.BootUsingImage=altimage
autoload.@entry[0]=entry
autoload.@entry[0].Configured=yes
autoload.@entry[0].SegmentName=altconfig
autoload.@entry[0].RemoteFilename=$$.ini
autoload.@entry[1]=entry
autoload.@entry[1].Configured=yes
autoload.@entry[1].SegmentName=altimage
autoload.@entry[1].RemoteFilename=$$.img
autoload.@entry[2]=entry
autoload.@entry[2].Configured=yes
autoload.@entry[2].SegmentName=config1
autoload.@entry[2].RemoteFilename=$$.vas
```

```
root@VA_router:/# uci export autoload
package 'autoload'

config 'core' 'main'
      option 'Enabled' "yes"
      option 'StartTimer' "10"
      option 'RetryTimer' "30"
      option 'NumberOfRetries' "5"
      option 'BackoffTimer' "15"
      option 'BootUsingConfig' "altconfig"
      option 'BootUsingImage' "altimage"

config 'entry'
      option 'Configured' "yes"
      option 'SegmentName' "altconfig"
      option 'RemoteFilename' "\$\$.ini"

config 'entry'
      option 'Configured' "yes"
      option 'SegmentName' "altimage"
      option 'RemoteFilename' "\$\$.img"

config 'entry'
      option 'Configured' "yes"
      option 'SegmentName' "config1"
      option 'RemoteFilename' "\$\$.vas"
```

9.2 Httpclient - Activator configuration

This section contains the settings for the http client used during activation and active updates of the device.

The httpclient core section configures the basic functionality of the module used for retrieving files from Activator during the Activation process. It contains the following settings.

Name	Type	Required	Default	Description
Enabled	boolean	yes	yes	Enables the http client.
list FileServer	integer	yes	none	Specifies the IP address of Activator that uses http port 80.

list SecureFileServer	integer	no	no	Specifies the IP address of Secure Activator that uses port 443.
ActivatorDownloadPath	string	yes	(none)	Specifies the url on Activator to which the client should send requests.
SecureDownload	boolean	no	no	Enables Secure Download (port 443).
PresentCertificate Enabled	boolean	no	no	Specifies if the client presents its certificate to the server to identify itself.
ValidateServer Certificate FieldEnabled	boolean	no	no	Specifies if the client validates the server certificate as per ServerCertificateField and FieldValueCertificateFormat
ServerCertificate Field	string	no	CN	Defines the field in the server certificate that the client should check.
ServerCertificate FieldValueCertificateFormat	string	no	PEM	Specifies the value the client expects to see in the specified field in the server certificate.

A sample httpclient configuration is shown below.

```
root@VA_router:~# uci show httpclient
httpclient.default=core
httpclient.default.Enabled=yes
httpclient.default.FileServer=10.1.83.36:80 10.1.83.37:80
httpclient.default.SecureFileServer=10.1.83.36:443 10.1.83.37:443
httpclient.default.ActivatorDownloadPath=/Activator/Sessionless/Httpserver.
asp
httpclient.default.SecureDownload=no
httpclient.default.PresentCertificateEnabled=no
httpclient.default.ValidateServerCertificateEnabled=no
httpclient.default.CertificateFile=/etc/httpclient.crt
httpclient.default.CertificateFormat=PEM
httpclient.default.CertificateKey=/etc/httpclient.key
root@VA_router:~# uci export httpclient
```

```
package httpclient

config core 'default'
        option Enabled 'yes'
        list FileServer '10.1.83.36:80'
        list FileServer '10.1.83.37:80'
        list SecureFileServer '10.1.83.36:443'
        list SecureFileServer '10.1.83.37:443'
        option ActivatorDownloadPath
'/Activator/Sessionless/Httpserver.asp'
        option SecureDownload 'no'
        option PresentCertificateEnabled 'no'
        option ValidateServerCertificateEnabled 'no'
        option CertificateFile '/etc/httpclient.crt'
        option CertificateFormat 'PEM'
        option CertificateKey '/etc/httpclient.key'
```

This sample contains the settings to enable the device to report its status to Monitor. To allow Monitor to track the IP address and ongoing presence of the device, a heartbeat SNMP trap is sent by default every minute.

Use the following settings to configure this feature.

Name	Type	Required	Default	Description
Enable	boolean	yes	no	Enables Monitor to send heartbeats.
interval_min	boolean	No	1	Specifies the interval at which traps are sent.
dev_reference	String	yes	(none)	Sets a unique identification for this device known to monitor.
monitor_ip	string	yes	(none)	Defines the IP address of Monitor. It is possible to specify multiple addresses to which SNMP heartbeat traps will be sent.

A sample Monitor configuration is shown below.

```
root@VA_router:~# uci show monitor
monitor.main=keepalive
monitor.main.enable=yes
monitor.main.interval_min=1
monitor.main.dev_reference=mikesamazondev
monitor.main.monitor_ip=10.1.83.36
root@VA_router:~# uci export monitor

package 'monitor'

config 'keepalive' 'main'
      option 'enable' "yes"
      option interval_min "1"
      option 'dev_reference' "mikesamazondev"
      list 'monitor_ip' "10.1.83.36"
```

9.3 System settings

The system section contains settings that apply to the most basic operation of the system, such as the host name, time zone, logging details, NTP server and language and web style.

This section details the configuration sections and parameters in various configuration files which are required to have the device perform basic routing activities on a network.

The system configuration contains basic settings for the whole router. Larger subsystems such as the network configuration, the DHCP and DNS server, and similar, have their own configuration file.

9.3.1 Configuring a router's host name

The host name appears in the top left hand of the menu of the interface. It also appears when you open a Telnet or SSH session.

Note: this document uses the hostname 'VA_router' throughout.

You can set your system setting options in the system section.

To configure the router's hostname, in the top menu, select **System -> system**. The System page appears.

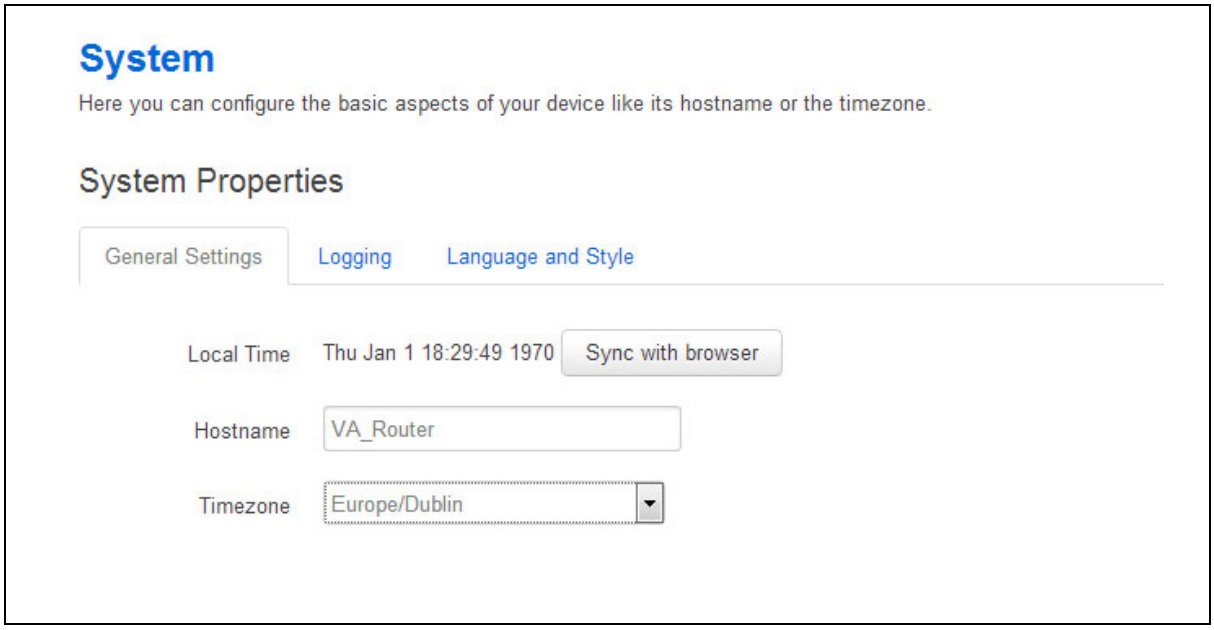


Figure 9: The system page

In the Hostname field, type a relevant host name.

In the Timezone dropdown menu, select the relevant time zone.

Click **Save**.

Name	Type	Required	Default	Description
hostname	string	no	(none)	Enables the hostname for this system.
buffersize	integer	no	kernel specific	Specifies the size of the kernel message buffer.
conloglevel	integer	no	7	Sets the maximum log level for kernel messages to be logged to the console. Only messages with a level lower than this will be printed to the console.
cronloglevel	integer	no	5	Specifies the minimum level for cron messages to be logged to syslog. 0 prints all debug messages; 8 will log command executions; and 9 or higher will only log error messages.
Klogconloglevel	integer	no	7	Specifies the maximum log level for kernel messages to be logged to the console. Only messages with a level lower than this will be printed to the console. Identical to

				conloglevel and will override it.
log_file	string	no	/var/log/messages	Defines which file to write log messages to (type file).
log_ip	IP address	no	(none)	Specifies IP address of a syslog server to which the log messages should be sent in addition to the local destination.
log_port	integer	no	514	Specifies port number of the remote syslog server specified with log_ip.
log_size	integer	no	16	Sets size of the file or circular memory buffer in KiB.
log_type	string	no	circular	Specifies either a circular or file log type.
timezone	string	no	UTC	Specifies the time zone that date and time should be rendered in by default.
time_save_interval_min	integer	no	10	Stores local time every N minutes so it will be used on the next boot.

The table below describes the fields in the Time Synchronization section.

Name	Type	Required	Default	Description
Enable builtin NTP server	Boolean	No	0	Enables NTP server
NTP update interval	Dropdown menu	No	2	Specifies interval of NTP requests
server	list of hostnames	no	(none)	Defines the pool of NTP servers to poll the time from. If the list is empty, the built in NTP daemon is not started.

A sample system configuration is shown below.

```
root@VA_router:~# uci show system
system.main=system
system.main.hostname=VA_router
system.main.timezone=UTC
system.main.log_ip=10.1.83.36
```

© Virtual Access 2015

```
system.main.log_port=514
system.main.password=admin

system.main.time_save_interval_min=10system.ntp=timeserver
system.ntp.interval_hours=2
system.ntp.server=0.openwrt.pool.ntp.org
package 'system'

config 'system' 'main'
      option 'hostname' "VA_router"
      option 'timezone' "UTC"
      option 'log_ip' "10.1.83.36"
      option 'log_port' "514"
      option 'password' "admin"
      option time_save_interval_min "10"
config 'timeserver' 'ntp'
      option interval_hours '2'
      list 'server' "0.VA_router.pool.ntp.org"
```

9.4 User management

9.4.1 Configuration file: config user

You can create different users on the system by defining them in the user management configuration file:

/etc/config/management_users

The following table describes the user's management configuration options.

Name	Type	Required	Default	Description
enabled	Boolean	Yes	0	Enables/creates the user.
username	Text	Yes	None	Defines username for the user.
password	Text	Yes	None	Defines password for the user.
webuser	Boolean	No	Yes	Specifies web access permissions for the user.
chapuser	Boolean	No	No	Specifies CHAP access permissions for the PPP connection.
Papuser	Boolean	No	No	Specifies PAP access permissions for the PPP connection.
srpuser	Boolean	No	No	Specifies SRP access permissions for the PPP connection.
smsuser	Boolean	No	No	Specifies SMS access permissions

				for the user.
linuxuser	Boolean	No	Yes	Specifies if access permissions for the user.

Note:

- webuser will only work if linuxuser is set to '**yes**'
- chapuser will only work if linuxuser is set to '**no**'

This first example shows a defined user called ‘test’. The user has a defined password ‘password’. They are also granted web access to the box.

```
root@VA_router:~# cat /etc/config/management_users
config user
        option enabled '1'
        option username 'test'
        option password 'password'
        option webuser 'yes'     option linuxuser 'yes'
```

This second example shows a user called ‘srptest’. The user has a defined password ‘srptest’.

```
config user
        option enabled '1'
        option username 'srptest'
        option password 'srptest'
        option srpuser '1'
        option chapuser '0'
        option webuser '0'

        option smsuser '0'
        option linuxuser 'no'
```

When the new user is defined, you must reboot the system for the changes to take effect.

After the reboot, the password option is replaced by a hash of the password. The hash password is now defined by the ‘hashpassword’ option.

For srpuser password will be defined by the ‘srphash’ option.

Note: when a new user is created on the system and given web access, they will no longer be able to login to the router web interface with the default root user details. The user must use the new login details.

9.4.2 UCI export and UCI show commands

Run UCI export or show commands to see management user UCI configuration settings.

```
root@VA_router:~# uci export management_users
package management_users
config user
        option enabled '1'
        option username 'test'
        option webuser 'yes'
        option linuxuser 'yes'
config user
        option enabled '1'
        option username 'srptest'
        option srpuser '1'
        option chapuser '0'
        option webuser '0'
        option smsuser '0'
        option linuxuser 'no'
        option srphash
'0:2de6Dk6D4tFo8oVfb2iuY6aRj2cAoPeo2DAdCRcReBUc.9Px56rNmamtaBx7BiQIzNisYFJF
VdhH6H0Z/Ys9RzU1SJrMVpmQZkJwqlB1tA.F7O.tf1VkGnXyiTLSCN68iJ.SltDDqeOprmLo/IW
9Ub7.qop44Ml3g6S5QJxpu.N5sLzpSvER.kAFNPR/DmK9D/.3SQzTtEZNYypmkgP9O2ihw/4uDU
NIFGMzd3dBs0VdF1AaFWNNqpAx7qP1JC4R5KeM/iGdo7lmKFyOTkvTIZbhXnWTRrQD5Q6nQv.UX
QrUmM4t3ztabT3gN.dibG3kNpMWl/DMLMBSghkXu7QosC:1uPbR5BbICQJFx'
root@VA_router:~# uci show management_users
management_users.@user[0]=user
management_users.@user[0].enabled=1
management_users.@user[0].username=test
management_users.@user[0].webuser=yes
management_users.@user[0].linuxuser=yes
management_users.@user[1]=user
management_users.@user[1].enabled=1
management_users.@user[1].username=srptest
management_users.@user[1].srpuser=1
management_users.@user[1].chapuser=0
management_users.@user[1].webuser=0
```

```
management_users.@user[1].smsuser=0
management_users.@user[1].linuxuser=no
management_users.@user[1].srphash=0:2de6Dk6D4tFo8oVfb2iuY6aRj2cAoPeo2DAdCRc
ReBUc.9Px56rNmamtaBx7BiQIzNisYFJFVdhH6H0Z/Ys9RzU1SJrMVpmQZkJwqlB1tA.F7O.tf1
VkGnXyiTLSCN68iJ.SltDDqeOprmLo/IW9Ub7.qop44Ml3g6S5QJxpu.N5sLzpSvER.kAFNPR/D
mK9D/.3SQzTtEZNYypmkgP9O2ihw/4uDUNIFGMzd3dBs0VdF1AaFWNNqpAx7qP1JC4R5KeM/iGd
o7lmKFyOTkvTIZbhXnWTRrQD5Q6nQv.UXQrUmM4t3ztabT3gN.dibG3kNpMWl/DMLMBSghkXu7Q
osC:1uPbR5BbICQJFx
```

Modify these settings by running uci set <parameter> command.

9.5 Interfaces configuration

This configuration is responsible for defining switch port groups, interface configurations and network routes.

Note: after changing the network configuration, to make your new configuration take effect, you need to execute the following:

/etc/init.d/network restart

There is no need to reboot the router.

Below is an overview of the section types that may be defined in the network configuration. A minimal network configuration for a router usually consists of at least two interfaces (LAN and WAN) and routes.

9.5.1 Interfaces

Sections of the type interface declare logical networks serving as container for IP address settings, aliases, routes, physical interface names and firewall rules, they play a central role within the overall configuration concept.

A minimal interface declaration consists of the following lines:

```
root@VA_router:~# uci show network.wan
network.wan=interface
network.wan.proto=dhcp
network.wan.ifname='eth0.1'
config 'interface' 'wan'
        option 'proto' 'dhcp'
        option 'ifname' 'eth0.1'
```

Wan is a unique logical interface name.

DHCP specifies the interface protocol, DHCP in this example eth0.1 is the physical interface associated with this section

The interface protocol may be one of the following shown in the table below.

Protocol	Description	Program
static	Static configuration with fixed address and netmask.	ip/ifconfig
dhcp	Address and netmask are assigned by DHCP.	udhcpc
3g	CDMA, UMTS or GPRS connection using an AT-style 3G modem.	comgt
L2tp	Layer 2 Tunneling Protocol.	xl2tpd
none	Unspecified protocol.	-

Depending on the interface protocol used, several other options may be required for a complete interface declaration. The corresponding options for each protocol are listed below. Options marked as "yes" in the "Required" column must be defined in the interface section if the corresponding protocol is used, options marked as "no" may be defined but can be omitted as well.

9.5.2 Options valid for all protocol types

Name	Type	Required	Default	Description
ifname	interface name(s)	yes	(none)	Defines physical interface name to assign to this section, list of interfaces if type bridge is set.
type	string	no	(none)	If set to "bridge", a bridge containing the given ifnames is created.
stp	boolean	no	0	Only valid for type "bridge", enables the Spanning Tree Protocol.
macaddr	mac address	no	(none)	Overrides MAC address of this interface.
mtu	number	no	(none)	Overrides the default MTU on this interface.
auto	boolean	no	0 for proto none, else 1	Specifies whether to bring up interface on boot.
accept_ra	boolean	no	1 for protocol dhcp, else 1	Specifies whether to accept IPv6 Router Advertisements on this interface.
send_rs	boolean	no	1 for protocol static, else 0	Specifies whether to send Router Solicitations on this interface.
monitored	Boolean	No	0	Specifies whether to send Interface status to Monitor.

9.5.3 Protocol "static"

Name	Type	Required	Default	Description
ipaddr	ip address	yes, if no ip6addr is set	(none)	Defines the IP address.
netmask	netmask	yes, if no ip6addr is set	(none)	Specifies Netmask.
gateway	ip address	no	(none)	Defines the default gateway.
broadcast	ip address	no	(none)	Defines broadcast address. Will be auto generated if not set.
ip6addr	ipv6 address	yes, if no ipaddr is set	(none)	Assign given IPv6 address to this interface (CIDR notation).
ip6gw	ipv6 address	no	(none)	Assign given IPv6 default gateway to this interface.
dns	list of ip addresses	no	(none)	Defines DNS server(s)'
metric	integer	no	0	Specifies the default route metric to use.

9.5.4 Protocol "dhcp"

Name	Type	Required	Default	Description
gateway	string	no	(none)	Supresses DHCP-assigned default gateway if set to 0.0.0.0.
broadcast	boolean	no	0	Enables the broadcast flag in DHCP requests, required for certain ISPs.
hostname	string	no	(none)	Specifies the hostname to include in DHCP requests.
clientid	string	no	system default	Overrides client identifier in DHCP requests.
vendorclass	string	no	system default	Overrides the vendor class in DHCP requests.
dns	list of ip addresses	no	(none)	Overrides DHCP-assigned DNS server(s).
metric	integer	no	0	Specifies the default route metric to use.
reqopts	list of strings	no	(none)	Specifies a list of additional DHCP options to request.

9.5.5 Protocol "3g" (PPP over EV-DO, CDMA, UMTS or GRPS)

Name	Type	Required	Default	Description
device	file path	yes	(none)	Specifies the modem device node /dev/ttyACM0.
service	string	yes	umts	Specifies the 3G service type:

				cdma/evdo, umts, gprs.
apn	string	yes	(none)	Sets the APN to use.
pincode	number	no	(none)	Sets the PIN code to unlock SIM card.
maxwait	number	no	20	Specifies the number of seconds to wait for modem to become ready.
username	string	no(?)	(none)	Sets the username for PAP/CHAP authentication.
password	string	no(?)	(none)	Sets the password for PAP/CHAP authentication.
keepalive	number	no	(none)	Specifies the number of connection failures before reconnect.
demand	number	no	(none)	Specifies the number of seconds to wait before closing the connection due to inactivity.
defaultroute	boolean	no	1	Replaces the existing default route on a PPP connect.
peerdns	boolean	no	1	Uses peer-assigned DNS server(s).
dns	list of ip addresses	no	(none)	Overrides peer-assigned DNS server(s).
ipv6	boolean	no	0	Enables IPv6 on the PPP link.

9.5.6 Protocol "l2tp" (layer 2 tunneling protocol)

Name	Type	Required	Default	Description
src_ipaddr	IPv4 address	yes	(none)	Defines the local IPv4 endpoint address.
server	IPv4 address	yes	(none)	Defines the remote IPv4 endpoint address.
user	string	yes	(none)	Sets the PPP user name.
password	string	yes	(none)	Sets the PPP password.
auth_mode	string	yes	(none)	Specifies Tunnel Authentication Mode: none: no authentication, unless secret is specified. simple: check peer hostname. challenge: require tunnel secret.
secret	string	no	(none)	Defines optional secret which is shared with tunnel peer.
persist	boolean	no	no	Recreates automatically if tunnel fails.
host_name	string	yes	(none)	Sets name to advertise to peer when setting up the tunnel.

9.5.7 Aliases

Use the Alias section to define further IPv4 and IPv6 addresses for interfaces. Alias sections also allow combinations like DHCP on the main interface and a static IPv6 address in the alias, for example to deploy IPv6 on WAN while

keeping normal internet connectivity. Each interface can have multiple aliases attached to it.

A minimal alias declaration consists of the following lines:

```
network.@alias[0]=alias
network.@alias[0].interface=lan
network.@alias[0].proto=static
network.@alias[0].ipaddr=10.0.0.1
network.@alias[0].netmask=255.255.255.0
config 'alias'
        option 'interface' 'lan'
        option 'proto' 'static'
        option 'ipaddr' '10.0.0.1'
        option 'netmask' '255.255.255.0'
```

Lan is the logical interface name of the parent interface.

Static is the alias interface protocol.

10.0.0.1 specifies the alias IP address.

255.255.255.0 specifies the alias netmask.

Only the static protocol type is allowed for aliases. Defined options for alias sections are listed below:

Name	Type	Required	Default	Description
interface	string	yes	(none)	Specifies the logical interface name of the parent (or master) interface this alias is belonging to, must refer to one of the defined interface sections.
proto	string	yes	(none)	Specifies the alias interface protocol must be static.
ipaddr	ip address	yes, if no ip6addr is set	(none)	Defines IP address.
netmask	netmask	yes, if no ip6addr is set	(none)	Defines Netmask.
gateway	ip address	no	(none)	Specifies the default gateway.
broadcast	ip address	no	(none)	Sets the broadcast address. This is auto generated if not set.
ip6addr	ipv6 address	yes, if noipaddr is set	(none)	IPv6 address (CIDR notation).
ip6gw	ipv6 address	no	(none)	IPv6 default gateway.
dns	list of ip	no	(none)	DNS server(s)

	addresses			
layer	integer	no	3	Selects the interface to attach to for stacked protocols (tun over bridge over eth, ppp over eth or similar). 3: attach to layer 3 interface (tun*, ppp* if parent is layer 3 else fallback to 2). 2: attach to layer 2 interface (br-* if parent is bridge else fallback to layer 1). 1: attach to layer 1 interface (eth*, wlan*). *any interface number, i.e 1, 2.

10 DHCP server and DNS configuration

Dynamic Host Configuration Protocol (DHCP) server is responsible for giving out IP addresses to hosts. IPs can be given out on different interfaces and different subnets. You can manually configure lease time as well as setting static IP to host mappings.

Domain Name Server (DNS) is responsible for resolution of IP addresses to domain names on the internet.

The dnsmasq program provides DHCP and DNS services. In the default configuration it contains one common section to specify DNS and daemon related options and one or more DHCP pools to define DHCP serving on network interfaces.

Possible section types of the DHCP configuration file are defined below. Not all types may appear in the file and most of them are only needed for special configurations. Common configurations are Common Options, DHCP Pools and Static Leases.

10.1 Common options section

The configuration section type dnsmasq determines values and options relevant to the overall operation of dnsmasq and the DHCP options on all interfaces served. The following table lists all available options, their default value, as well as the corresponding dnsmasq command line option.

These are the default settings for the common options:

```
root@VA_router:~# uci show dhcp
dhcp.@dnsmasq[0]=dnsmasq
dhcp.@dnsmasq[0].domainneeded=1
dhcp.@dnsmasq[0].boguspriv=1
dhcp.@dnsmasq[0].filterwin2k=0
dhcp.@dnsmasq[0].localise_queries=1
dhcp.@dnsmasq[0].rebind_protection=1
dhcp.@dnsmasq[0].rebind_localhost=1
dhcp.@dnsmasq[0].local=/lan/
dhcp.@dnsmasq[0].domain=lan
dhcp.@dnsmasq[0].expandhosts=1
dhcp.@dnsmasq[0].nonegcache=0
dhcp.@dnsmasq[0].authoritative=1
dhcp.@dnsmasq[0].readethers=1
```

```
dhcp.@dnsmasq[0].leasefile=/tmp/dhcp.leases
dhcp.@dnsmasq[0].resolvfile=/tmp/resolv.conf.auto
dhcp.@dnsmasq[0].interface=lan
config 'dnsmasq'
      option domainneeded      1
      option boguspriv  1
      option filterwin2k       0
      option localise_queries  1
      option rebind_protection 1
      option rebind_localhost  0
      option local             '/lan/'
      option domain            'lan'
      option expandhosts       1
      option nonegcache        0
      option authoritative     1
      option readethers        1
      option leasefile  '/tmp/dhcp.leases'
      option resolvfile        '/tmp/resolv.conf.auto'
      list interface 'lan'
```

Options `local` and `domain` enable dnsmasq to serve entries in `/etc/hosts` as well as the DHCP client's names as if they were entered into the lan DNS domain.

Options `domainneeded`, `boguspriv`, `localise_queries`, and `expandhosts` make sure that requests for these local host names (and the reverse lookup) never get forwarded to the upstream DNS servers.

Option `authoritative` makes the router the only DHCP server on this network. This allows clients to get their IP lease a lot faster.

Name	Type	Required	Default	Description
addnhosts	list of file paths	no	(none)	Specifies additional host files to read for serving DNS responses.
authoritative	boolean	no	0	Forces dnsmasq into authoritative mode, this speeds up DHCP leasing. Used if this is the only server in the network.
Boguspriv	boolean	no	0	Rejects reverse lookups to private IP ranges where no corresponding entry exists in

				/etc/hosts.
Cachelocal	boolean	no	1	When set to 0, uses each network interface's dns address in the local /etc/resolv.conf. Normally, only the loopback address is used, and all queries go through dnsmasq.
cachesize	integer	no	150	Sets the size of dnsmasq query cache.
dhcp_boot	string	no	(none)	Specifies BOOTP options, in most cases just the file name.
dhcphostsfile	file path	no	(none)	Specifies an external file with per host DHCP options.
dhcpleasemax	integer	no	150	Specifies the maximum number of DHCP leases.
dnsforwardmax	integer	no	150	Specifies the maximum number of concurrent connections.
domain	domain name	no	(none)	Specifies the DNS domain handed out to DHCP clients.
domainneeded	boolean	no	0	Tells dnsmasq to never forward queries for plain names, without dots or domain parts, to upstream nameservers. If the name is not known from /etc/hosts or DHCP then a "not found" answer is returned.

Option `leasefile` stores the leases in a file, so that they can be picked up again if dnsmasq is restarted.

Option `resolvfile` tells dnsmasq to use this file to find upstream name servers; it is created by the WAN DHCP client or the PPP client.

Name	Type	Required	Default	Description
ednspacket_max	integer	no	1280	Specifies the largest EDNS.0 UDP packet which is supported by the DNS forwarder.
enable_tftp	boolean	no	0	Enables the built in TFTP server.
expandhosts	boolean	no	0	Adds the local domain part to names found in /etc/hosts
filterwin2k	boolean	no	0	Does not forward requests that cannot be answered by public name servers.
interface	list of interface names	no	(all interfaces)	Specifies a list of interfaces to listen on. If unspecified, dnsmasq will listen to all interfaces except those listed in

				not interface.
leasefile	file path	no	(none)	Stores DHCP leases in this file.
Local	string	no	(none)	Looks up DNS entries for this domain from /etc/hosts. This follows the same syntax as server entries, see the man page.
localise_queries	boolean	no	0	Chooses IP address to match the incoming interface if multiple addresses are assigned to a host name in /etc/hosts.
logqueries	boolean	no	0	Logs the results of DNS queries, dump cache on SIGUSR1.
nodaemon	boolean	no	0	Does not daemonize the dnsmasq process.
Nohosts	boolean	no	0	Does not read DNS names from /etc/hosts.
nonegcache	boolean	no	0	Disables caching of negative "no such domain" responses.
noresolv	boolean	no	0	Does not read upstream servers from /etc/resolv.conf.
notinterface	list of interface names	no	(none)	Interfaces dnsmasq should not listen on. Note: individual interface sections will be appended if ignore is set there.
nonwildcard	boolean	no	0	Only listens on configured interfaces, instead of on the wildcard address.
Port	port number	no	53	Defines listening port for DNS queries, disables DNS server functionality if set to 0.
queryport	integer	no	(none)	Uses a fixed port for outbound DNS queries.
readethers	boolean	no	0	Reads static lease entries from /etc/ethers, re-read on SIGHUP.
Resolvfile	file path	no	/etc/ resolv. conf	Specifies an alternative resolv file.
server	list of strings	no	(none)	Specifies list of DNS servers to forward requests to. See the dnsmasq man page for syntax details.
strictorder	boolean	no	0	Obeys order of DNS servers in /etc/resolv.conf.
tftp_root	directory path	no	(none)	Specifies the TFTP root directory.
rebind_protection	boolean	no	1	Enables DNS rebind attack protection by discarding upstream RFC1918 responses.
rebind_localhost	boolean	no	0	Allows upstream 127.0.0.0/8

				responses, required for DNS based blacklist services, only takes effect if rebind protection is enabled.
rebind_domain	list of domain names	no	(none)	Specifies a list of domains to allow RFC1918 responses for, only takes effect if rebind protection is enabled.

10.2 DHCP pools

Sections of the type dhcp specify per interface lease pools and settings for serving DHCP requests. Typically there is at least one section of this type present in the/etc/config/dhcp file to cover the LAN interface.

You can disable a lease pool for a specific interface by specifying the ignore option in the corresponding section.

A minimal example of a dhcp section is shown below.

```
root@VA_router:~# uci show dhcp.lan
dhcp.lan=dhcp
dhcp.lan.interface=lan
dhcp.lan.start=100
dhcp.lan.limit=150
dhcp.lan.leasetime=12h
dhcp.lan.ignore=1

config 'dhcp' 'lan'
      option 'interface'   'lan'
      option 'start'       '100'
      option 'limit'        '150'
      option 'leasetime'   '12h'
```

Lan specifies the VA_router interface that is served by this DHCP pool.

100 is the offset from the network address, in the default configuration 192.168.1.100.

150 is the maximum number of addresses that may be leased, in the default configuration 192.168.1.250.

12h specifies the time to live for handed out leases, twelve hours in the example below.

Name	Type	Required	Default	Description
dhcp_option	list of strings	no	(none)	Enables additional options to be added for this network-id. For example with '26,1470' or 'option:mtu, 1470' you can assign an MTU per DHCP. Your client must accept MTU by DHCP for this to work.
dynamicdhcp	boolean	no	1	Dynamically allocates client addresses, if set to 0 only clients present in the ethers files are served.
force	boolean	no	0	Forces DHCP serving on the specified interface even if another DHCP server is detected on the same network segment.
ignore	boolean	no	0	Specifies whether dnsmasq should ignore this pool if set to 1.
Interface	logical interface name	yes	(none)	Specifies the interface associated with this DHCP address pool, must be one of the defined interfaces in/etc/config/network.
Leasetime	string	yes	12h	Specifies the lease time of addresses handed out to clients, for example 12h or30m.
Limit	integer	yes	150	Specifies the maximum allowable address that may be leased to clients. It is calculated as network address + "start" + "limit".
networkid	string	no	(value of interface)	Assigns a network-id to all clients that obtain an IP address from this pool.
start	integer	yes	100	Specifies the offset from the network

				address of the underlying interface to calculate the minimum address that may be leased to clients. It may be greater 255 to span subnets.

10.3 Static leases

You can assign fixed IP addresses to hosts on your network, based on their MAC (hardware) address.

The configuration options in this section are used to construct a –G option for dnsmasq.

```
root@VA_router:~# uci show dhcp.mypc
dhcp.mypc=host
dhcp.mypc.ip=192.168.1.2
dhcp.mypc.mac=00:11:22:33:44:55
dhcp.mypc.name=mypc

config host 'mypc'
        option ip       '192.168.1.2'
        option mac      '00:11:22:33:44:55'
        option name     'mypc'
This adds the fixed IP address 192.168.1.2 and the name "mypc" for a
machine with the (Ethernet) hardware address 00:11:22:33:44:55
```

	Type	Required	Default	Description
ip	string	yes	(none)	Specifies the IP address to be used for this host.
mac	string	yes	(none)	Specifies the hardware address of this host.
name	string	no	(none)	Sets the optional hostname to assign.

11 VLAN configuration

11.1 VLAN web interface

You can configure VLANs through three sections:

- Native VLAN
- VLAN Definition
- Port Description
- Native VLAN

Figure 10: The native VLAN section

The Native VLAN section specifies the native VLAN to be used. This VLAN will be sent untagged across the trunk link.

Note: you must create the VLAN before setting it as native.

Name	Type	Required	Default	Description
802.1Q VLAN ID	Numeric value	No	Blank	VLAN ID number defines VLAN that will be sent across the trunk untagged. NO 802.IQ tag will be applied to the packets on that VLAN.

Table 4: Native VLAN field name and description

11.2 VLAN definition

Use the VLAN definition section to define VLANs and assign them with VLAN ID, name and required network configurations.

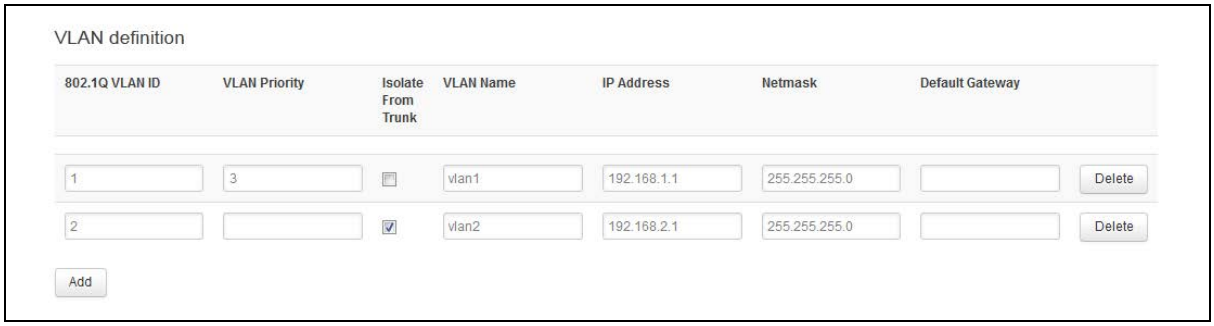


Figure 11: The VLAN definition section

Name	Type	Required	Default	Description
802.1Q VLAN ID	Numeric value	No	Blank	Defines VLAN number. The VLAN will be referred to using this number.
VLAN Priority	Numeric value	No	Blank	Specifies 802.1p VLAN priority tag on trunk links.
Isolate From Trunk	Boolean	No	Blank	Defines whether to isolate hosts from each other within the same VLAN. Hosts will still be able to communicate with the router.
VLAN Name	Text	Yes	Blank	Configures VLAN name.
IP Address	IP Address	Yes	Blank	Configures network mask address to be used on this VLAN.
Netmask	IP Address	Yes	Blank	Configures network mask address to be used on this VLAN.
Default Gateway	IP Address	No	Blank	Configures default gateway address to be used on this VLAN.

Table 5: VLAN definition fields and their descriptions

11.3 Port description

The port description section is used to segment the switch accordingly to your VLAN requirements. You can specify what physical ports you want to assign to which VLANs, or whether you want to configure a trunk port instead.

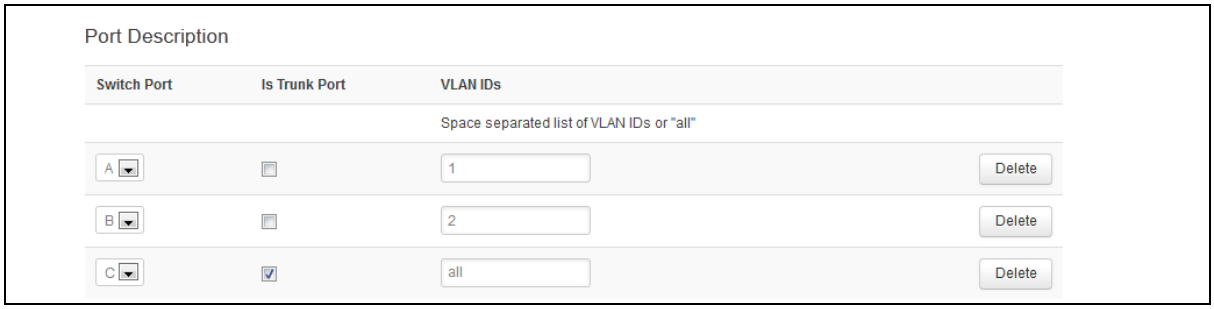


Figure 12: The port description section

Name	Type	Required	Default	Description
Switch Port	Text	Yes	Blank	Specifies which physical port on the front panel of the router will be assigned to which VLAN.
Is Trunk Port	Boolean	NO	Blank	Configures the port as a trunk port.
VLAN IDs	Numeric value/text	Yes	Blank	Specifies what VLANs will be assigned to a physical port on the router. You must use VLAN ID to specify which VLANs or 'all' to configure a port as trunk interface.

Table 6: The port description fields and their descriptions

11.4 VLANs UCI interface

You can configure VLANs through CLI.

The VLAN configuration file is stored at:

/etc/config/portvlan

```
~# uci export portvlan
package portvlan

config vlan
        option vlanid '1'
        option name 'vlan1'
        option ipaddr '192.168.1.1'
        option netmask '255.255.255.0'
        option isolate 'no'

config vlan
        option vlanid '2'
        option name 'vlan2'
        option ipaddr '192.168.2.1'
        option netmask '255.255.255.0'
        option vlanprio '5'
        option isolate 'yes'

config port
        option port 'A'
        option vlans '1'

config port
        option port 'B'
        option vlans '2'
config port
        option port 'C'
        option trunk 'yes'
        option vlans 'all'
config nat_vlan 'nat_vlan'
        option nat_vlanid '1'
```

```
root@VA_router:~# uci show portvlan
portvlan.@vlan[0]=vlan
portvlan.@vlan[0].vlanid=1
portvlan.@vlan[0].name=vlan1
portvlan.@vlan[0].ipaddr=192.168.1.1
portvlan.@vlan[0].netmask=255.255.255.0
portvlan.@vlan[0].isolate=no
portvlan.@vlan[1]=vlan
portvlan.@vlan[1].vlanid=2
portvlan.@vlan[1].name=vlan2
portvlan.@vlan[1].ipaddr=192.168.2.1
portvlan.@vlan[1].netmask=255.255.255.0
portvlan.@vlan[1].vlanprio=5
portvlan.@vlan[1].isolate=yes
portvlan.@port[0]=port
portvlan.@port[0].port=A
portvlan.@port[0].vlans=1
portvlan.@port[1]=port
portvlan.@port[1].port=B
portvlan.@port[1].vlans=2
portvlan.@port[2].port=C
portvlan.@port[2].trunk=yes
portvlan.@port[2].vlans=all
portvlan.nat_vlan=nat_vlan
portvlan.nat_vlan.nat_vlanid=1
```

Modify these settings by running uci set <parameter> command.

The following tables describe the UCI parameters for each section.

11.4.1 config port

Name	Type	Required	Default	Description
port	Text	Yes	Blank	Specifies which physical port on the front panel of the router will be assigned to which VLAN
trunk	Boolean	No	Blank	Configures the port as a trunk port.
vlans	Numeric value/text	Yes	Blank	Specifies what VLANs will be assigned to a physical port on the router. You must use VLAN ID to specify which VLANs or 'all' to configure a port as trunk interface.

11.4.2 config vlan

Name	Type	Required	Default	Description
vlanid	Numeric value	No	Blank	Defines VLAN number. The VLAN will be referred to using this number.
vlanprio	Numeric value	No	Blank	Specifies 802.1p VLAN priority tag on trunk links.
Isolate	Boolean	No	Blank	Defines whether to isolate hosts from each other within the same VLAN. Hosts will still be able to communicate with the router.
name	Text	Yes	Blank	Configures VLAN name.
ipaddr	IP Address	Yes	Blank	Configures network mask address to be used on this VLAN.
netmask	IP Address	Yes	Blank	Configures network mask address to be used on this VLAN.

11.4.3 Config nat vlan

Name	Type	Required	Default	Description
Nat vlanid	Numeric value	No	Blank	VLAN ID number. Defines VLAN that will be sent across the trunk untag

12 Static routes configuration

Static routes can be added to the routing table to forward traffic to specific subnets when dynamic routing protocols are not used or they are not configured for such subnets. They can be created based on outgoing interface or next hop IP address.

12.1 IPv4 routes

It is possible to define arbitary IPv4 routes on specific interfaces using route sections. As for aliases, multiple sections can be attached to an interface. These kind or routes are most commonly known as static routes.

A minimal example is shown below:

```
network.name_your_route=route
network.name_your_route.interface=lan
network.name_your_route.target=172.16.123.0
network.name_your_route.netmask=255.255.255.0
network.name_your_route.gateway=172.16.123.100

config 'route' 'name_your_route'
        option 'interface' 'lan'
        option 'target' '172.16.123.0'
        option 'netmask' '255.255.255.0'
        option 'gateway' '172.16.123.100'
```

Lan is the logical interface name of the parent interface.

172.16.123.0 is the network address of the route.

255.255.255.0 specifies the route netmask.

Legal options for IPv4 routes are described in the table below.

Name	Type	Required	Default	Description
interface	string	yes	(none)	Specifies the logical interface name of the parent (or master) interface this route is belonging to, must refer to one of the defined interface sections.
target	ip address	yes	(none)	Specifies the network address.
netmask	netmask	no	(none)	Defines route netmask. If omitted, 255.255.255.255 is assumed which makes the target a host address.
Gateway	ip address	no	(none)	Network gateway. If omitted, the gateway from the parent interface is taken. If set to 0.0.0.0 no gateway will be specified for the

				route.
metric	number	no	0	Specifies the route metric to use.
mtu	number	no	interface MTU	Defines a specific MTU for this route.

12.2 IPv6 routes

IPv6 routes can be specified as well by defining one or more route6 sections.

A minimal example is shown below.

```
network.@route6[0]=route6
network.@route6[0].interface=lan
network.@route6[0].target=2001:0DB8:100:F00:BA3::1/64
network.@route6[0].gateway=2001:0DB8:99::1

config 'route6'
        option 'interface' 'lan'
        option 'target' '2001:0DB8:100:F00:BA3::1/64'
        option 'gateway' '2001:0DB8:99::1'
```

Lan is the logical interface name of the parent interface.

2001:0DB8:100:F00:BA3::1/64 is the routed IPv6 subnet in CIDR notation.

2001:0DB8:99::1 specifies the IPv6 gateway for this route.

Legal options for IPv6 routes are:

Name	Type	Required	Default	Description
interface	string	yes	(none)	Specifies the logical interface name of the parent (or master) interface this route is belonging to, must refer to one of the defined interface sections.
target	ipv6 address	yes	(none)	Sets the IPv6 network address.
gateway	ipv6 address	no	(none)	Sets the IPv6 gateway. If omitted, the gateway from the parent interface is taken.
metric	number	no	0	Specifies the route metric to use.
mtu	number	no	interface MTU	Defines a specific MTU for this route.

Dropbear is the software module that implements ssh on the system. The dropbear section contains these settings:

Name	Type	Required	Default	Description
enable	boolean	no	1	Enables dropbear.Set to **0** to disable starting dropbear at system boot.
verbose	boolean	no	0	Enables verbose. Set to **1** to enable verbose output by the start script.
BannerFile	string	no	(none)	Specifies the name of a file to be printed before the user has authenticated successfully.
PasswordAuth	boolean	no	1	Specifies password authentication. Set to **0** to disable authenticating with passwords.
Port	integer	no	22	Specifies the port number to listen on.
RootPasswordAuth	boolean	no	1	Enables root password authentication. Set to **0** to disable authenticating as root with passwords.
RootLogin	boolean	no	1	Enables root logins. Set to **0** to disable SSH logins as root.
GatewayPorts	boolean	no	(none)	Enables gateway ports. Set to **1** to allow remote hosts to connect to forwarded ports.
Interface	string	no	(none)	Tells dropbear to listen only on the specified interface.
Identity	string	no	SSH-2.0-dropbear_2013.60	Sets alternative name that appears for dropbear version

13 BGP (Border Gateway Protocol)

13.1 Configuring the BGP web interface

In the top menu, select **Network -> BGP**. BGP configuration page appears.

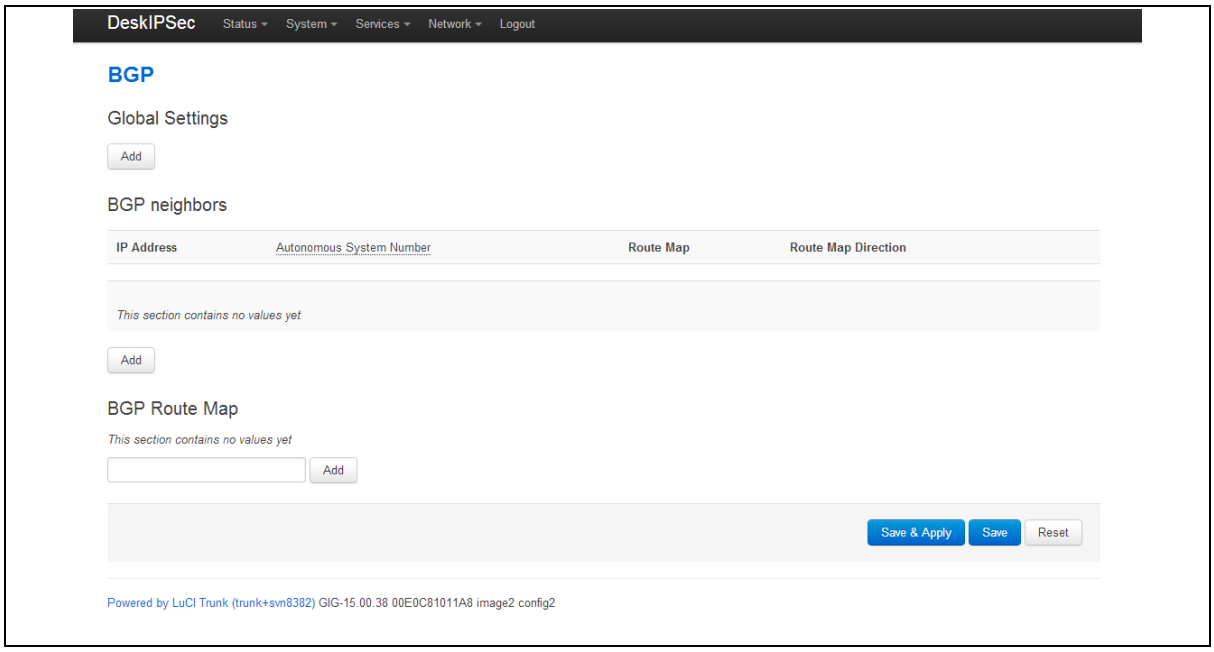


Figure 13: BGP page

To configure global BGP settings, click **Add**.

Figure 14: BGP global settings page

Name	Type	Required	Default	Description
BGP Enabled	Check box	Yes	Unchecked	Enables BGP protocol.
Router ID	Integer	Yes	None	Sets Unique Router ID in format 4

				byte format 0.0.0.0.
Autonomous System Number	Integer	Yes	None	Defines ASN for local router.
Network	Integer	Yes	None	Sets network that will be advertised to neighbours in prefix format 0.0.0.0/0. Ensure network prefix matches the one shown in routing table. See Routes section below.

When you have made your changes, click **Save**.

13.2 Optionally configure BGP route map

To configure the BGP route map, on the Global Settings page scroll down to the BG Route Map section.

Figure 15: The BGP route map section

Type in a name for the BGP Route map Name and then click **Add**. The ROUTEMAP configuration section appears.

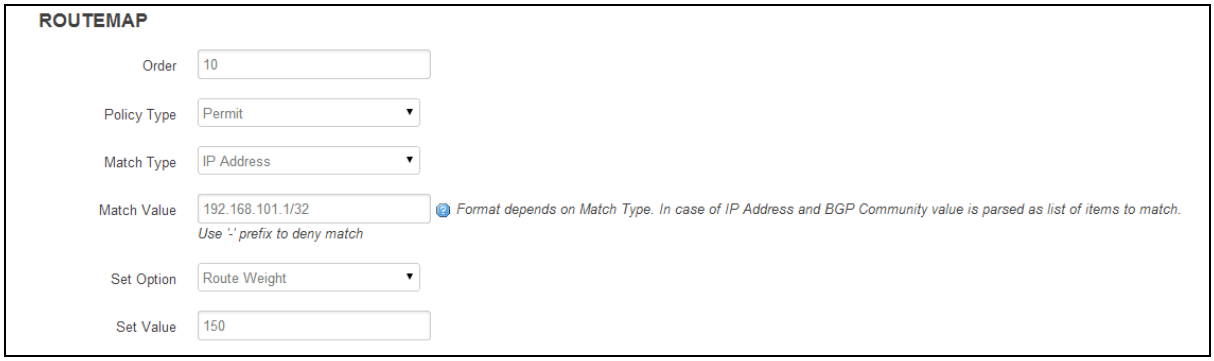


Figure 16: The routemap section

Name	Type	Required	Default	Description
Order	Integer	Yes	None	Route Map sequence number
Policy Type	Dropdown Menu	Yes	Permit	Permits or denies matched values
Match Type	Dropdown Menu	Yes	IP address	Available options are: IP Address, IP Next-Hop, AS-Path, Route Metric, BGP Community
Match Value		Yes	None	Format depends on Match Type. In

				case of IP address and BGP Community values is parsed as list of items to match.
Set Option	Dropdown Menu	No	None	Available options are: None, IP Next Hop, Local Preference, MED, Route Weight, BGP MED, AS path to Prepend, BGP Community.
Set Value				Format depends on the Set Option chosen.

When you have made your changes, click **Save**.

13.3 Configure BGP neighbours

In the BGP neighbours section, click **Add** to configure BGP neighbours.

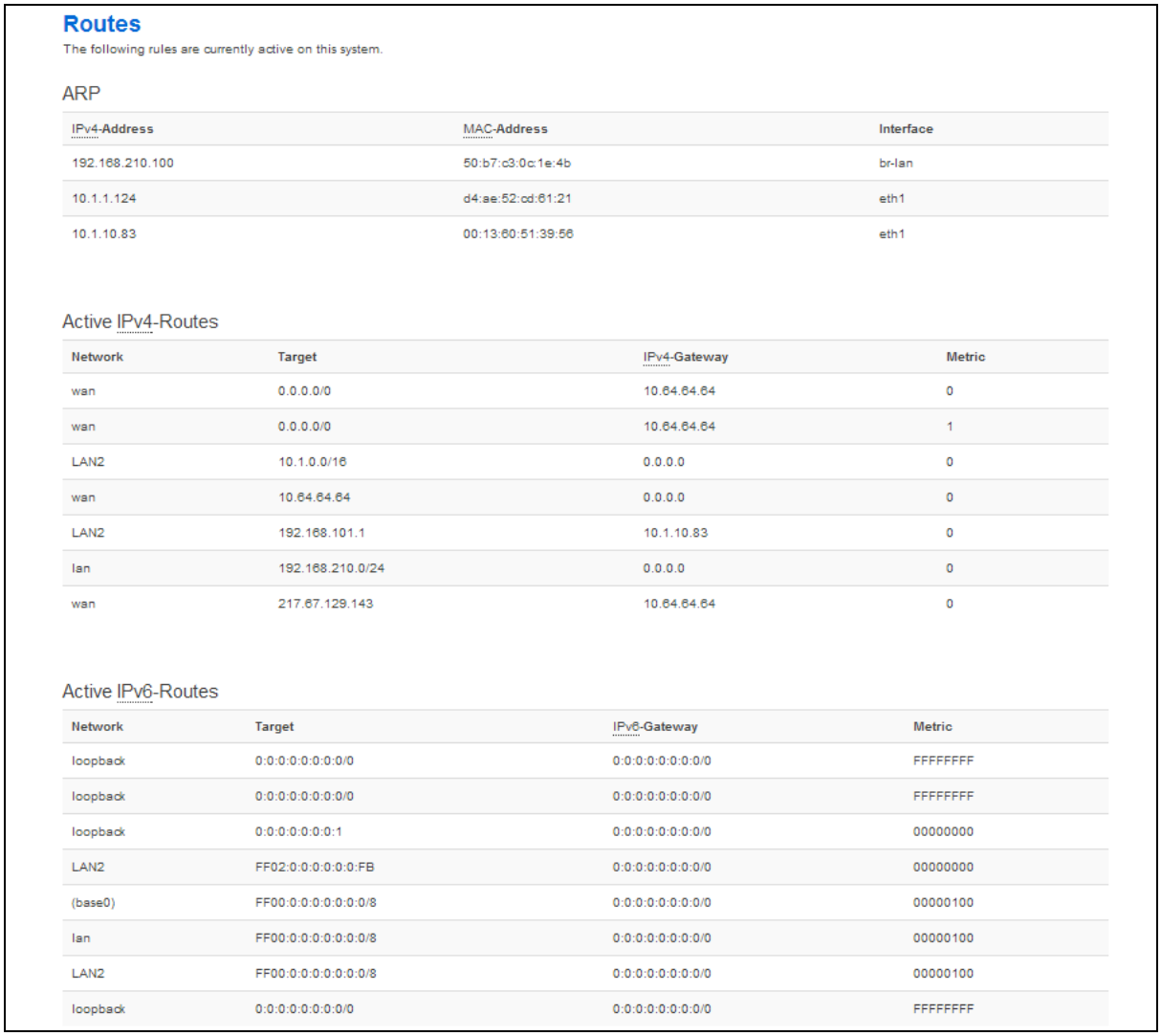
Figure 17: The BGP neighbours section

Name	Type	Required	Default	Description
IP Address	Integer	Yes	None	Sets the IP address of the neighbour.
Autonomous System Number	Integer	Yes	None	Sets the ASN of the remote peer.
Route Map	String	No	None	Sets the route map name.
Route Map Direction	Dropdown Menu	No	None	Tells in which direction the route map should be applied. Available options are: in or out.

Click **Save & Apply**.

13.4 Routes statistics

To view routes statistics, in the top menu click **Status -> Routes**. The routing table appears.



Routes

The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address	Interface
192.168.210.100	50:b7:c3:0c:1e:4b	br-lan
10.1.1.124	d4:ae:52:cd:61:21	eth1
10.1.10.83	00:13:60:51:39:56	eth1

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric
wan	0.0.0.0/0	10.64.64.64	0
wan	0.0.0.0/0	10.64.64.64	1
LAN2	10.1.0.0/16	0.0.0.0	0
wan	10.64.64.64	0.0.0.0	0
LAN2	192.168.101.1	10.1.10.83	0
lan	192.168.210.0/24	0.0.0.0	0
wan	217.67.129.143	10.64.64.64	0

Active IPv6-Routes

Network	Target	IPv6-Gateway	Metric
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF
loopback	0:0:0:0:0:0:0:1	0:0:0:0:0:0:0:0/0	00000000
LAN2	FF02:0:0:0:0:0:0:FB	0:0:0:0:0:0:0:0/0	00000000
(base0)	FF00:0:0:0:0:0:0:0/8	0:0:0:0:0:0:0:0/0	00000100
lan	FF00:0:0:0:0:0:0:0/8	0:0:0:0:0:0:0:0/0	00000100
LAN2	FF00:0:0:0:0:0:0:0/8	0:0:0:0:0:0:0:0/0	00000100
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF

Figure 18: The routing table

13.5 BGP UCI interface

You can also configure BGP UCI through CLI using the UCI command suite.

The configuration file is stored at:

/etc/config/bgpd

To view the configuration file, use the commands:

uci export bgpd

or

uci show bgpd

```
package bgpd

config routing 'bgpd'
        option enabled 'yes'
        option router_id '3.3.3.3'
        option asn '1'
        list network '11.11.11.0/29'
        list network '192.168.103.1/32'

config peer
        option route_map_in 'yes'
        option ipaddr '11.11.11.1'
        option asn '1'
        option route_map 'ROUTEMAP'

config routemap 'ROUTEMAP'
        option order '10'
        option permit 'yes'
        option match_type 'ip address'
        option match '192.168.101.1/32'
        option set_type 'ip next-hop'
        option set '150'

root@VA_router:~# uci show bgpd
bgpd.bgpd=routing
bgpd.bgpd.enabled=yes
bgpd.bgpd.router_id=3.3.3.3
bgpd.bgpd.asn=1
bgpd.bgpd.network=11.11.11.0/29 192.168.103.1/32
bgpd.@peer[0]=peer
bgpd.@peer[0].route_map_in=yes
bgpd.@peer[0].ipaddr=11.11.11.1
bgpd.@peer[0].asn=1
bgpd.@peer[0].route_map=ROUTEMAP
bgpd.ROUTEMAP=routemap
bgpd.ROUTEMAP.order=10
```

```
bgpd.ROUTEMAP.permit=yes
bgpd.ROUTEMAP.match_type=ip address
bgpd.ROUTEMAP.match=192.168.101.1/32
bgpd.ROUTEMAP.set_type=ip next-hop
bgpd.ROUTEMAP.set=150
```

To change any of the above values use `uci set` command

14 Configuring WiFi

This section explains how to configure WiFi on a Virtual Access router using the web interface or via UCI.

14.1 Configuring WiFi through the web interface

WiFi can act as an Access Point (AP) to another device in the network or it can act as a client to an existing AP.

You can configure WiFi in AP mode in two different ways:

- on an existing interface, or
- on a new interface.

14.2 Configuring WiFi in AP mode on an existing Ethernet interface

In the top menu, select **Network -> Interfaces**. The Interface Overview page appears.

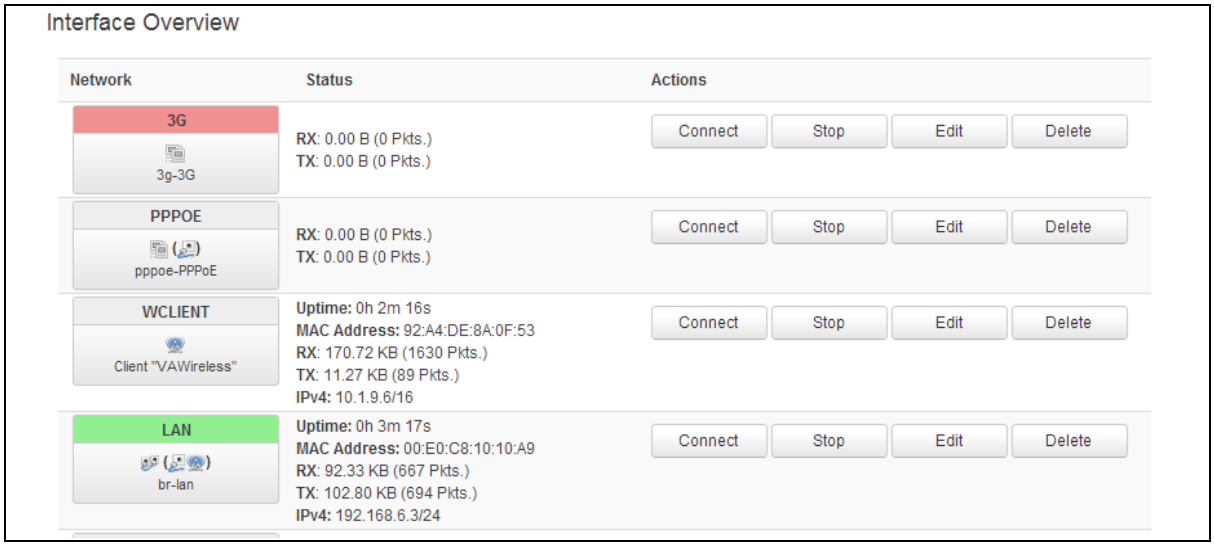


Figure 19: The interface overview page

In the interface overview page, click **Edit** to select the Ethernet interface that will be bridged into the router's WiFi AP. The Common Configuration page appears.

In the Common Configuration page select the **Physical Settings** tab.

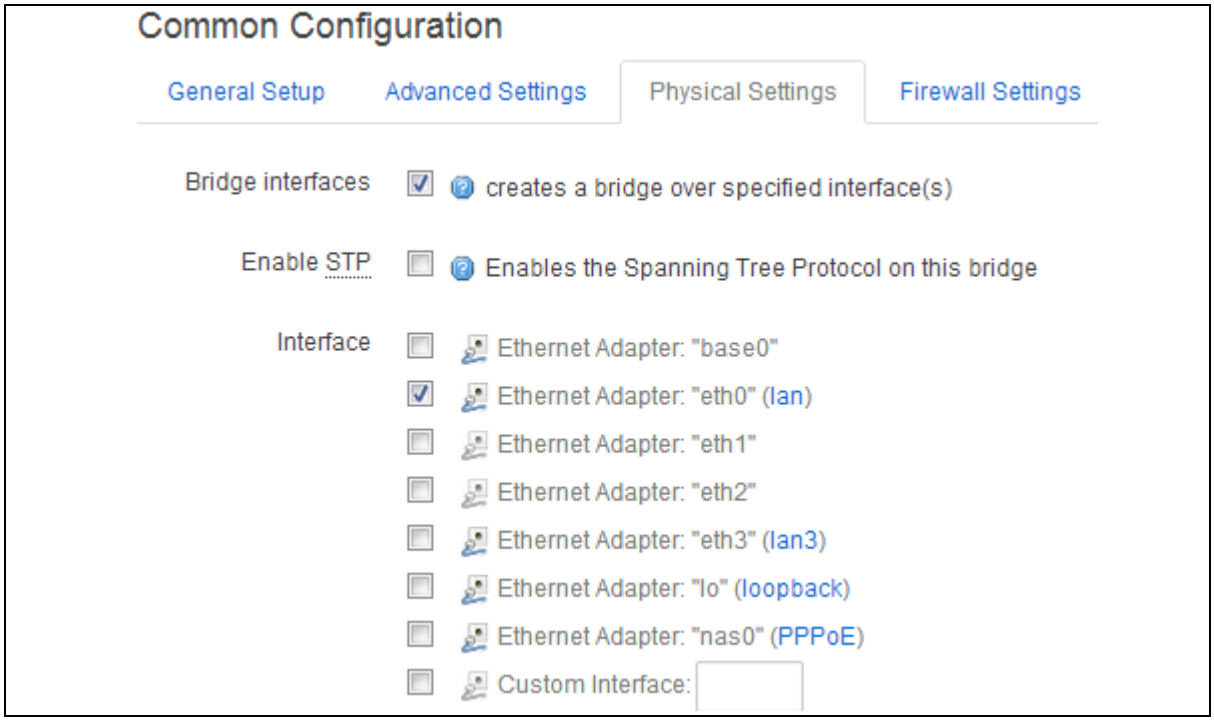


Figure 20: The common configuration physical settings page

Select **Bridge Interfaces**.

In the Interface fields, you will see the interface that you are working on is already selected.

Name	Type	Required	Default	Description
Bridge Interfaces	Check box	Yes	Unchecked	Creates a bridge over specified interfaces.
Enable STP	Check box	Yes	Unchecked	Enables STP
Interface	Check box	N/A	Unchecked	Selects the interface for WiFi.

Scroll to the bottom of the page and click **Save**.

In the top menu, select **Network -> WiFi**. The Wireless Overview page appears.

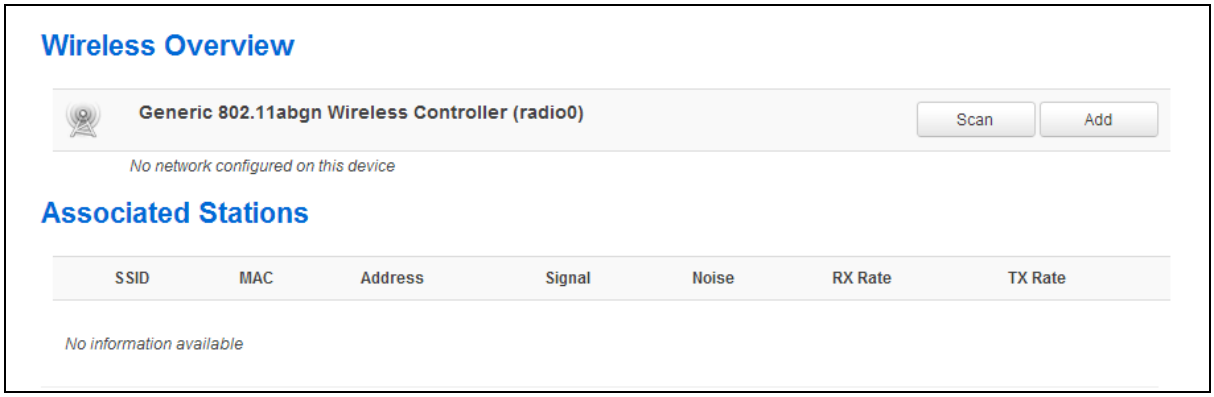


Figure 21: The wireless overview page

To create a new WiFi interface, click **Add**. The Wireless Network page appears.

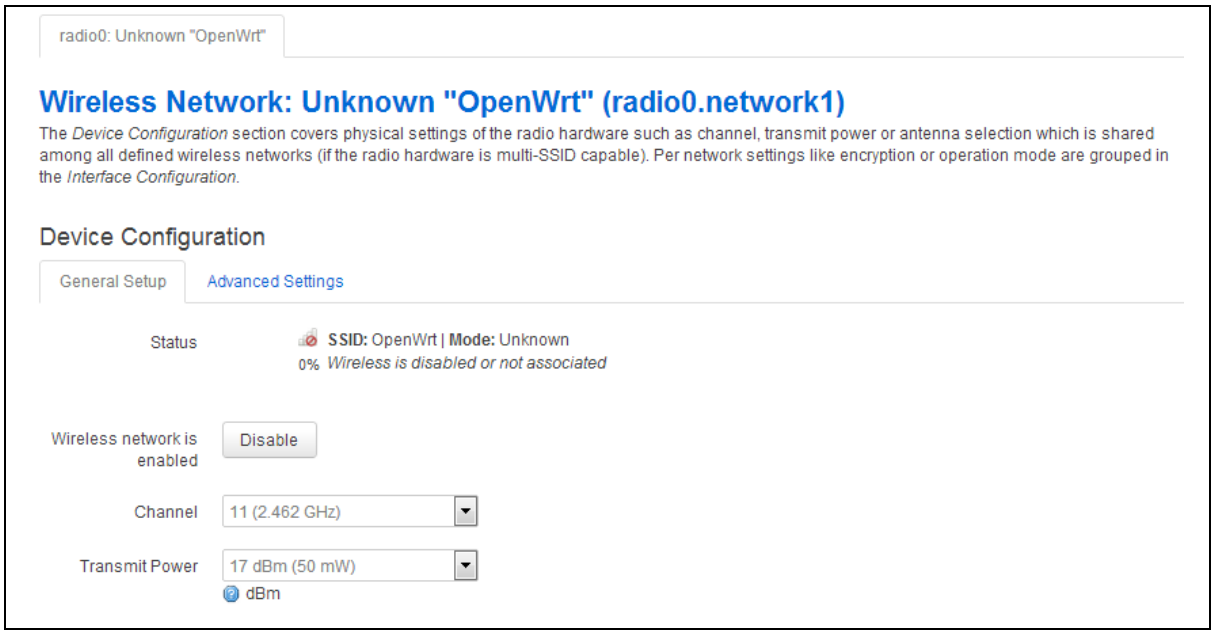

radio0: Unknown "OpenWrt"
Wireless Network: Unknown "OpenWrt" (radio0.network1)
The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which is shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the Interface Configuration.
Device Configuration
General Setup
Advanced Settings
Status
SSID: OpenWrt | Mode: Unknown
0% Wireless is disabled or not associated
Wireless network is enabled
Disable
Channel
11 (2.462 GHz)
Transmit Power
17 dBm (50 mW)
dBm

Figure 22: The wireless network page

In the Device Configuration section, ensure you have selected the **General Setup** tab.

In the Channel drop down menu, select the **channel** you require.

In the Transmit Power drop down menu, select the power rating you require.

Name	Type	Required	Default	Description
Channel	Drop down menu	Yes	11(2.462 GHz)	Available channels are within range 1-11
Transmit Power	Drop down menu	Yes	17 dBm (50 mW)	Available range 0 dBm(1 mW) – 17dBm(50 mW)

Scroll down to the Interface Configuration section.

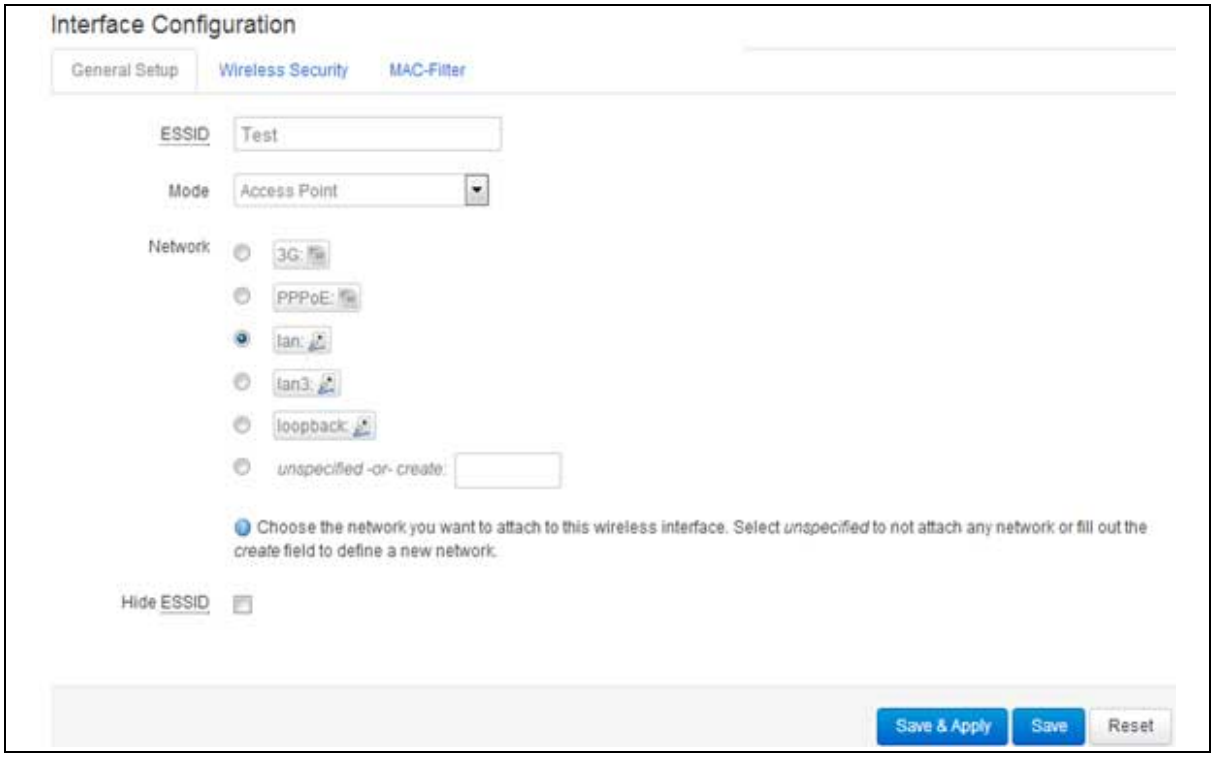


Figure 23: The interface configuration page

Ensure you have selected the **General Setup** tab.

In the ESSID field, type **[name of the wireless local area network]**.

In the Mode drop down menu, select **Access Point**.

Select one of the Ethernet interfaces to which the WiFi AP mode will be bridged.

Name	Type	Required	Default	Description
ESSID	Drop down menu	Yes	Blank	Extended Service Set Identification. The name of the wireless local area network
Mode	Drop down menu	Yes	Access Point	Selects Access Point mode.

Click **Save**.

Select the **Wireless Security** tab.

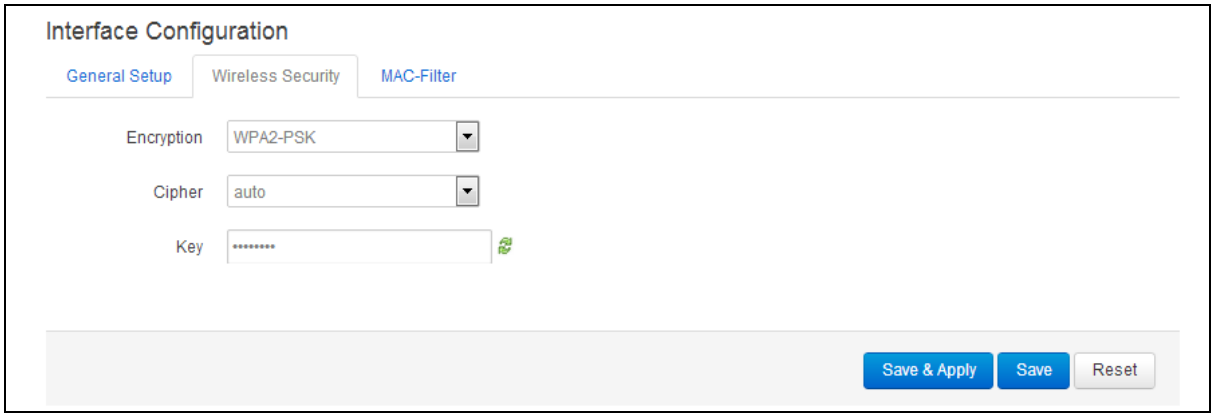


Figure 24: The interface configuration page

In the Encryption drop down menu, select the **encryption key**.

In the Cipher drop down menu, select the **cipher type**.

Create an encryption key.

Click **Save & Apply**.

14.3 Configuring WiFi in AP mode on a new interface

In the top menu, select **Network -> Wifi**. The Wireless Overview page appears.

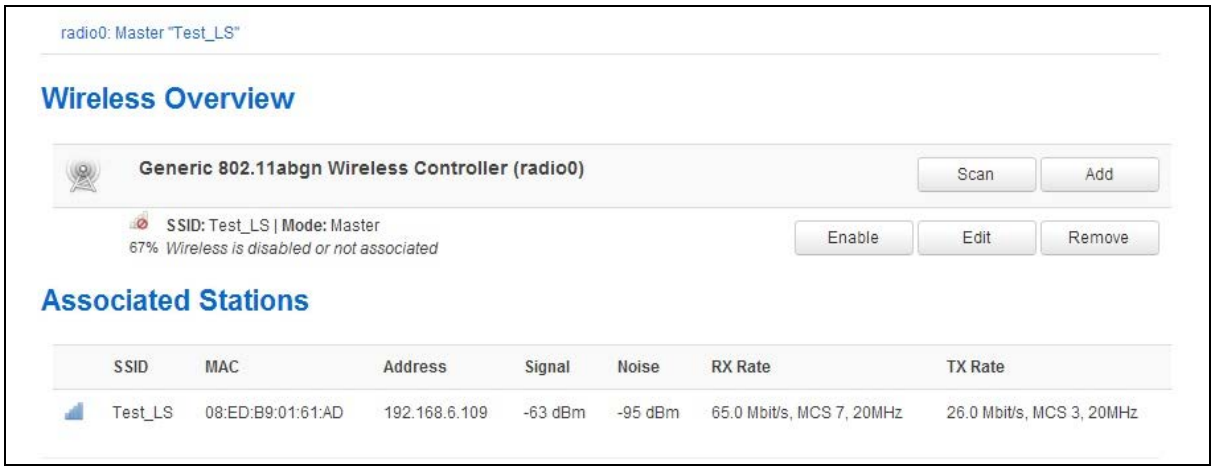


Figure 25: The wireless overview page

Click **Add** to create a new WiFi interface.

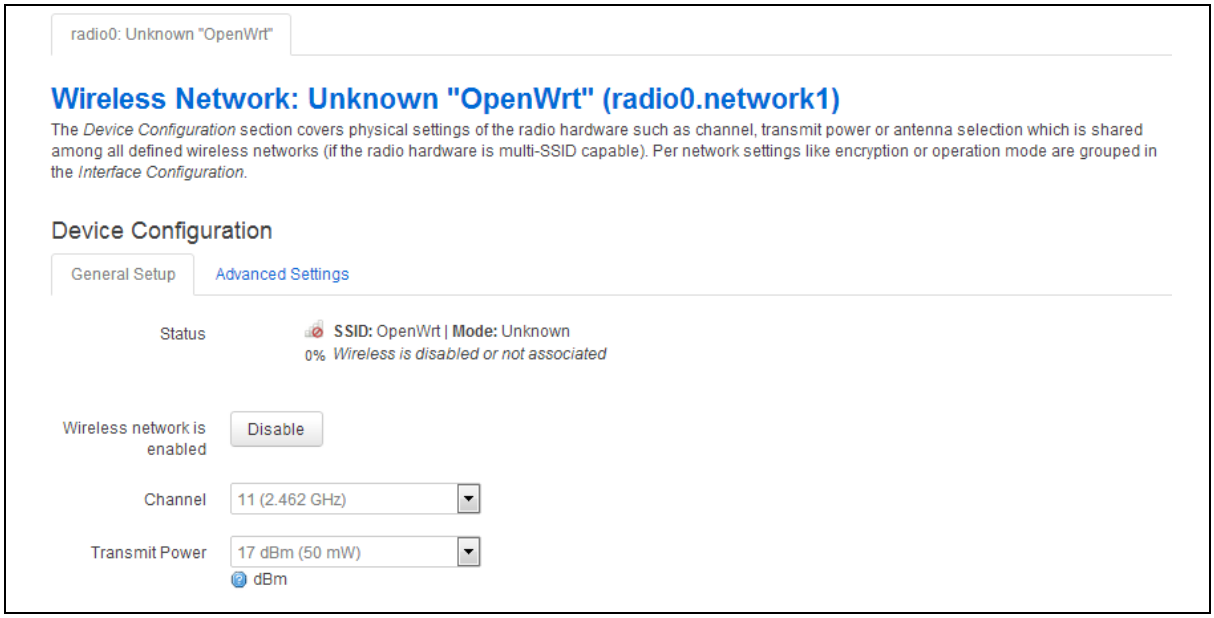

radio0: Unknown "OpenWrt"
Wireless Network: Unknown "OpenWrt" (radio0.network1)
The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which is shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the Interface Configuration.
Device Configuration
General Setup
Advanced Settings
Status
SSID: OpenWrt | Mode: Unknown
0% Wireless is disabled or not associated
Wireless network is enabled
Disable
Channel
11 (2.462 GHz)
Transmit Power
17 dBm (50 mW)
dBm

Figure 26: The wireless network page

In the Device Configuration section, ensure the **General Setup** tab is selected.

In the Channel drop down menu, select the **channel** you require.

In the Transmit Power drop down menu, select the **power rating** you require.

Name	Type	Required	Default	Description
Channel	Drop down menu	Yes	11 (2.462 GHz)	Available channels are within range 1-11
Transmit Power	Drop down menu	Yes	17 dBm (50 mW)	Available range 0 dBm(1 mW) – 17dBm(50 mW)

In the Interface Configuration section, make sure you have selected the **General Setup** tab.

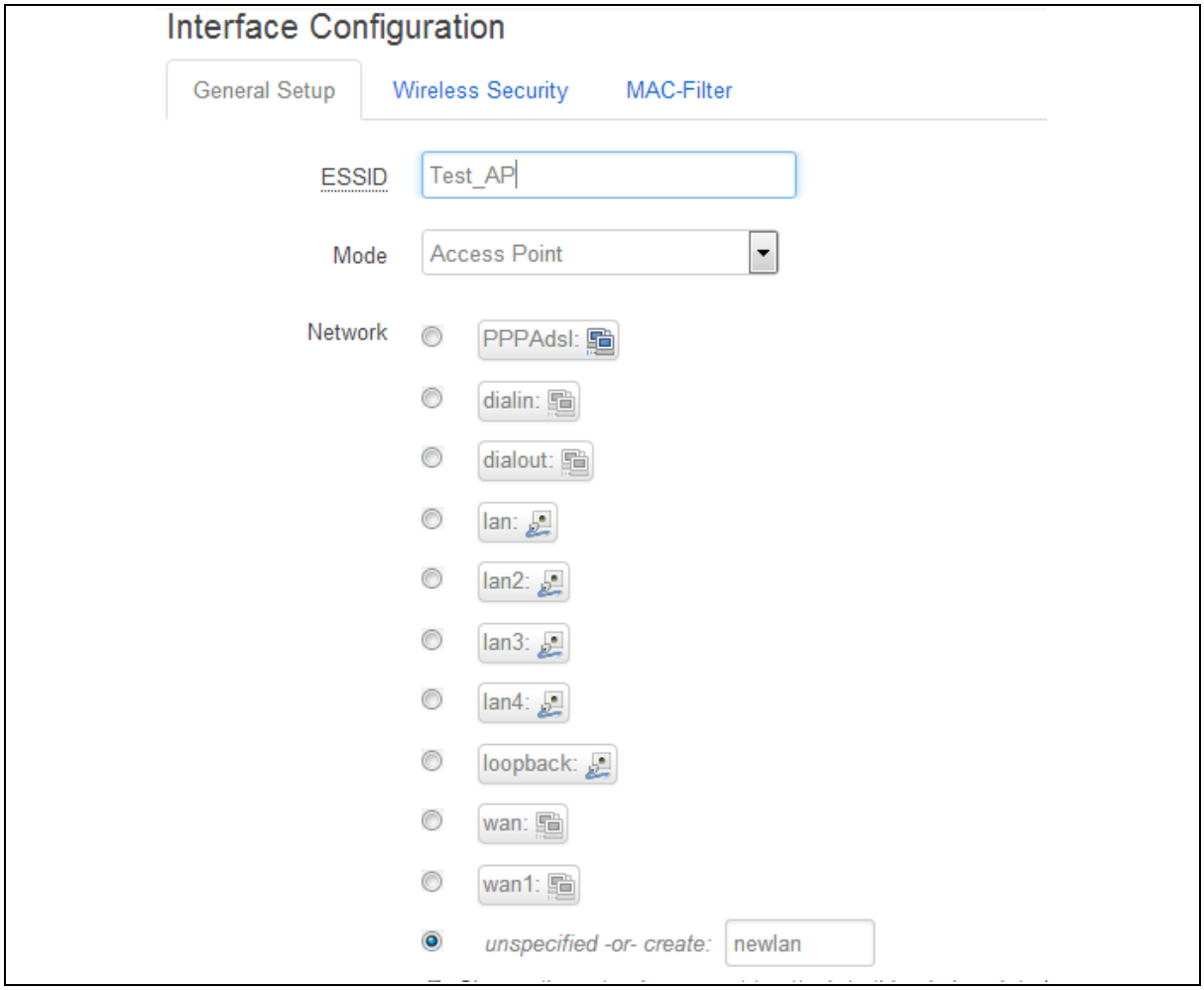


Figure 27: The general set up tab

In the ESSID field, type **[name of the wireless local area network]**.

In the Mode drop down menu, select **Access Point**.

In the unspecified –or- create: field, type the **name of the new WiFi interface**.

Name	Type	Required	Default	Description
ESSID	Drop down menu	Yes	Blank	Extended Service Set Identification. The name of the wireless local area network
Mode	Drop down menu	Yes	Access Point	Selects Access Point mode.

Select the **Wireless Security tab**.

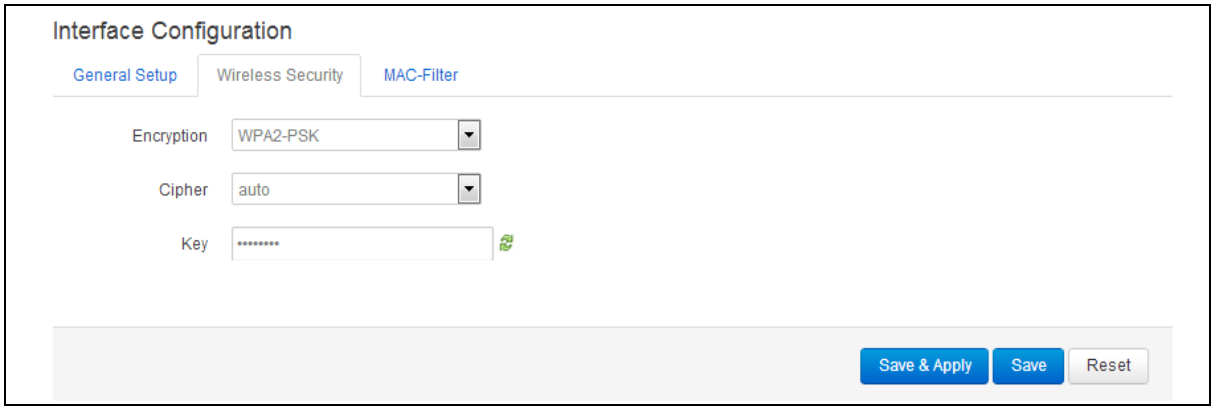


Figure 28: The wireless security tab

In the Encryption drop down menu, select the **encryption key**. When you have entered the encryption type, the Cipher and Key fields appear.

In the Cipher drop down menu, select the **cipher type**.

Create an encryption key.

Click **Save**.

In the top menu, select **Network -> Interfaces**. The Interfaces Overview page appears.

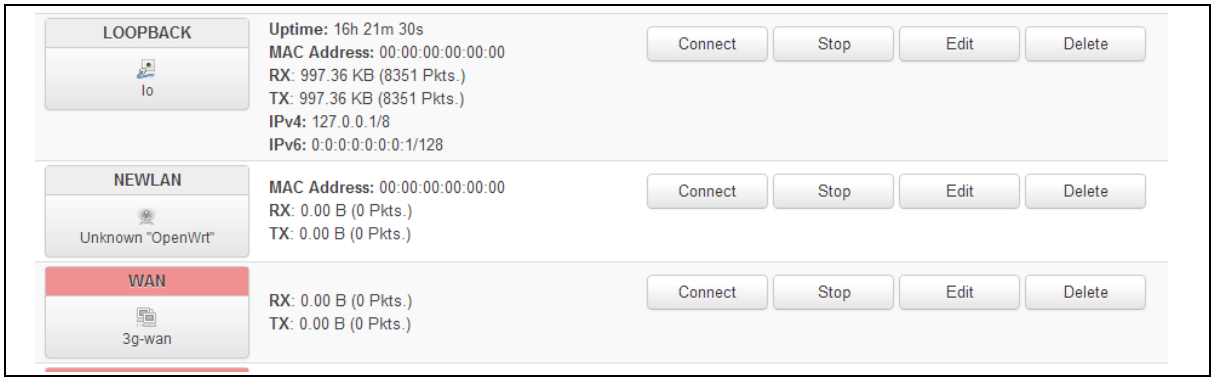


Figure 29: The interface overview page showing the newly created interface

Click **Edit** on the newly created interface.

Ensure you have selected the **General Setup** tab.

In the Protocol drop down menu, select **Static Address**. A 'Switch Protocol' button appears.

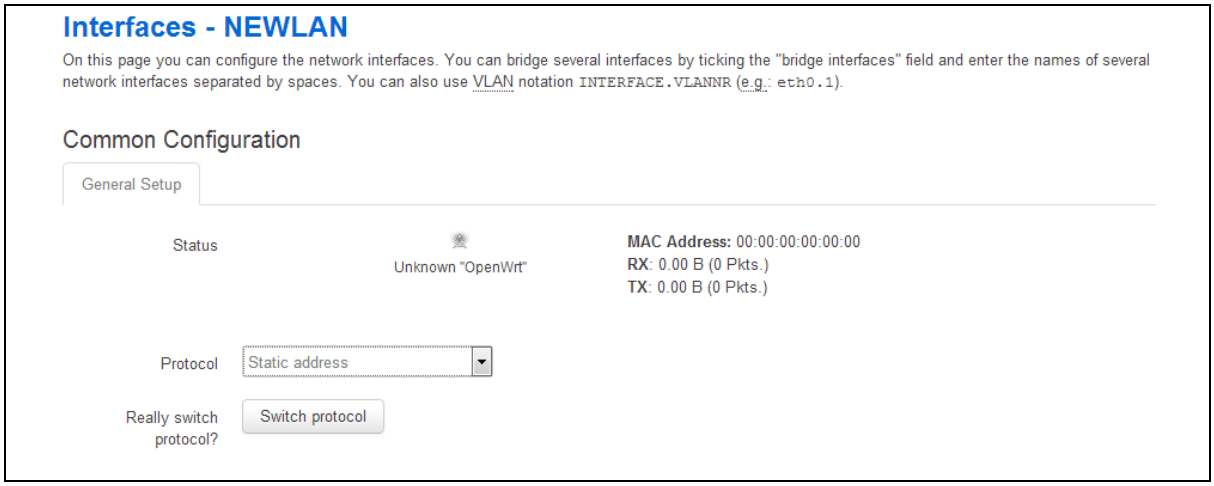

Interfaces - NEWLAN
On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).
Common Configuration
General Setup
Status
Unknown "OpenWrt"
MAC Address: 00:00:00:00:00:00
RX: 0.00 B (0 Pkts.)
TX: 0.00 B (0 Pkts.)
Protocol
Static address
Really switch protocol?
Switch protocol

Figure 30: The new interface page showing protocol button

Click **Switch Protocol**. The new interface configuration page appears.

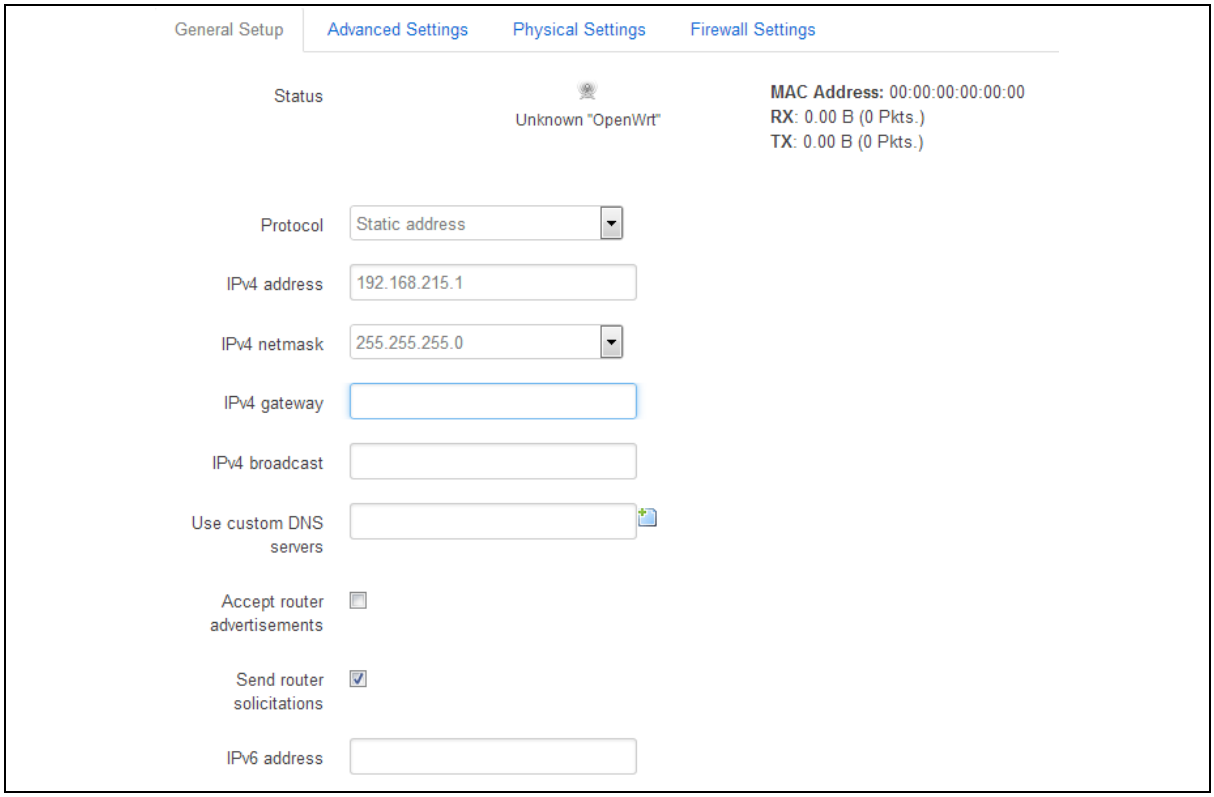


Figure 31: The new interface page

Name	Type	Required	Default	Description
Protocol	Drop down menu	Yes	Static Address	
IPv4 address	Numeric Value	Yes	N/A	IP address assigned to this interface
IPv4 netmask	Numeric Value	Yes	N/A	IP netmask assigned to this interface

IPv4 gateway	Numeric Value	No	N/A	
IPv4 broadcast	Numeric Value	No	N/A	
Use custom DNS servers	String	No	N/A	DNS server IP address
Accept router advertisements	Check box	No	N/A	
Send router solicitations	Check box	No	N/A	

Type in the **Static IP address**.

Type in the **Network Mask**.

Click **Save & Apply**.

Note: The router will now start the network package. It may take up to one minute for connectivity to the router to be restored.

14.4 Configuring WiFi in client mode

In the top menu, select **Network ->Wifi**. The Wireless Overview page appears.

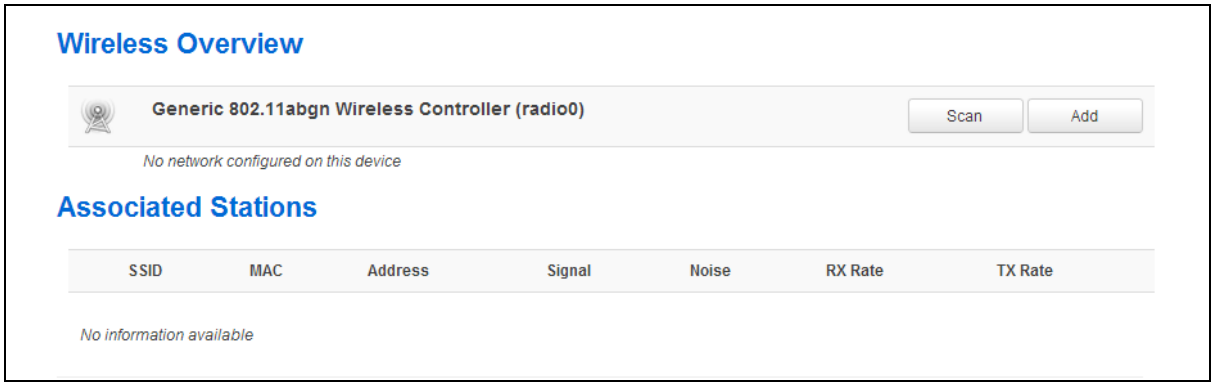


Figure 32: The wireless overview page

Click **Add** to create a new WiFi Client interface. The Wireless Network page appears.

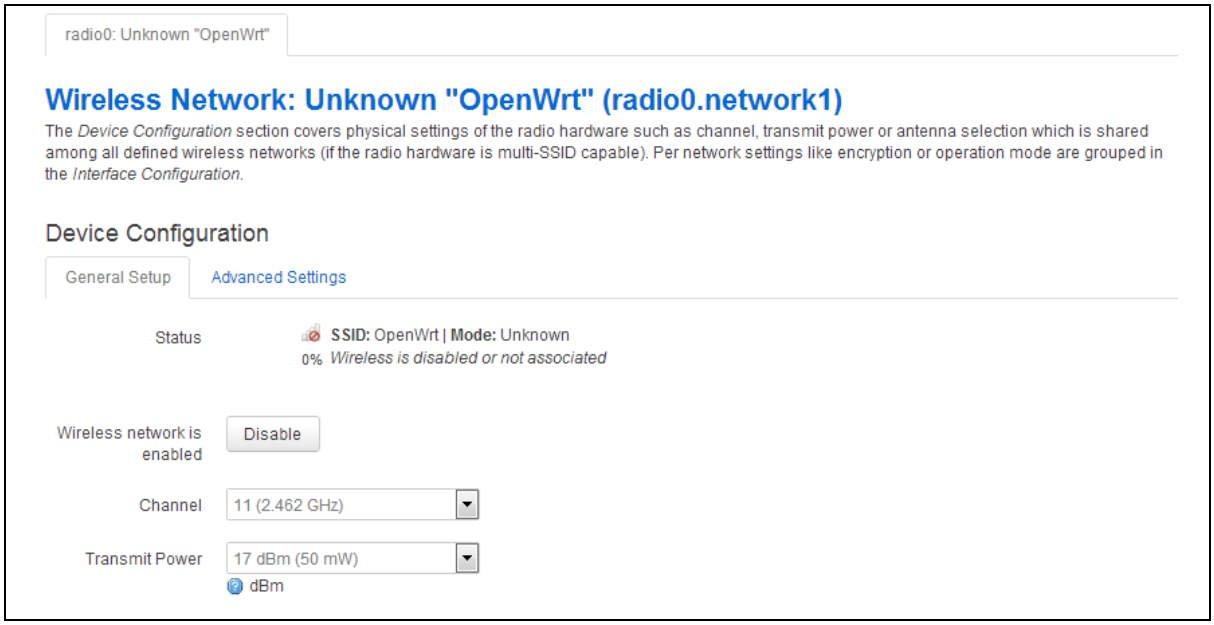

radio0: Unknown "OpenWrt"
Wireless Network: Unknown "OpenWrt" (radio0.network1)
The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which is shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the Interface Configuration.
Device Configuration
General Setup
Advanced Settings
Status
SSID: OpenWrt | Mode: Unknown
0% Wireless is disabled or not associated
Wireless network is enabled
Disable
Channel
11 (2.462 GHz)
Transmit Power
17 dBm (50 mW)
dBm

Figure 33: The wireless network page

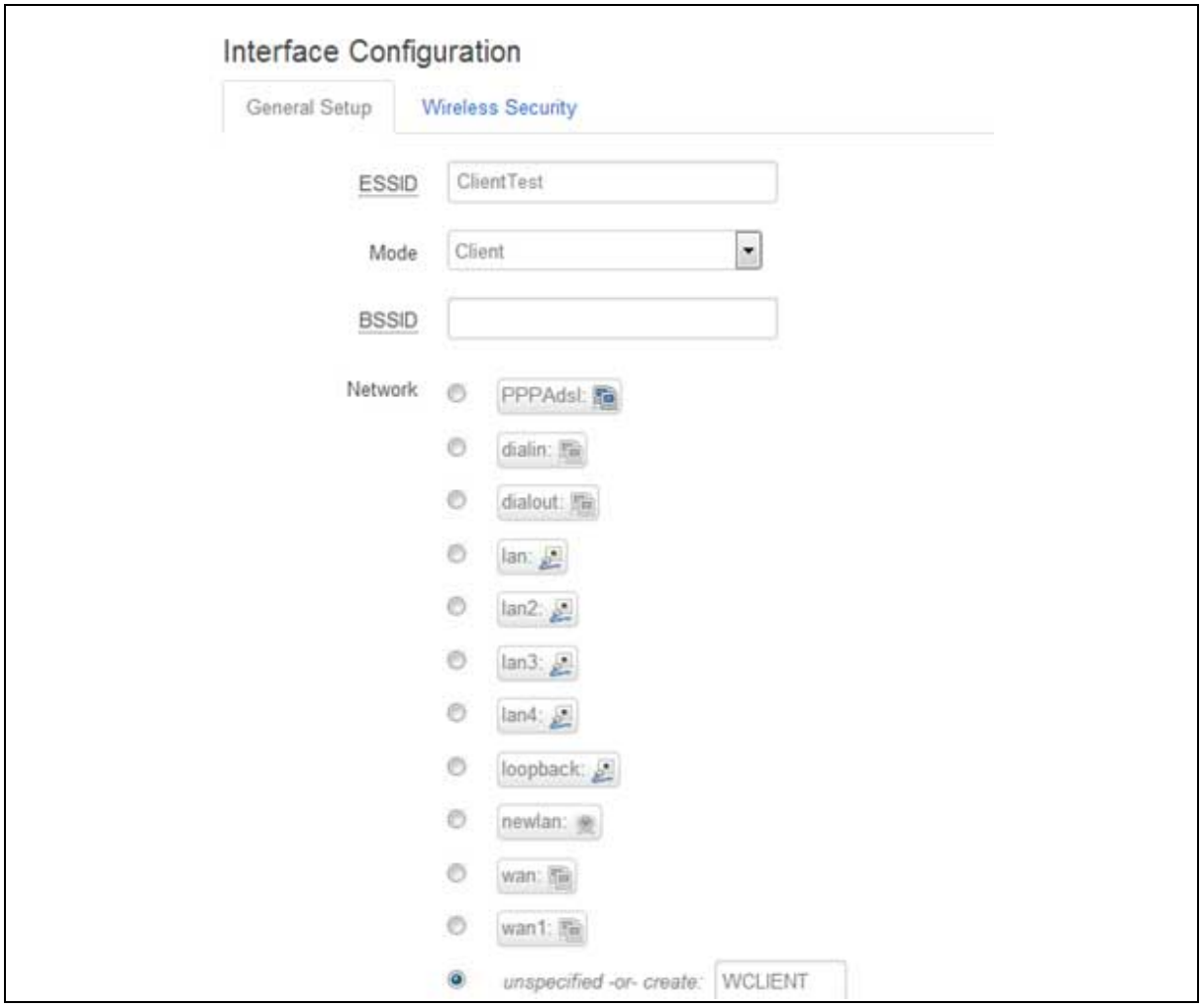
In the Device Configuration section, ensure you have selected the **General Setup** tab.

In the Channel drop down menu, select the **channel** you require.

In the Transmit Power drop down menu, select the **power rating** you require.

Name	Type	Required	Default	Description
Channel	Drop down menu	Yes	11 (2.462 GHz)	Available channels are within range 1-11
Transmit Power	Drop down menu	Yes	17 dBm (50 mW)	Available range 0 dBm(1 mW) – 17dBm(50 mW)

In the Interface Configuration section, make sure you have selected the **General Setup** tab.



In the ESSID field, type **[name of the wireless local area network]**.

In the Mode drop down menu, select **Client**.

In the unspecified –or- create: field, type the name of the **new WiFi interface**.

Name	Type	Required	Default	Description
ESSID	Drop down menu	Yes	Blank	Extended Service Set Identification. The name of the wireless local area network
Mode	Drop down menu	Yes	Access Point	Selects mode.

Select the **Wireless Security** tab.

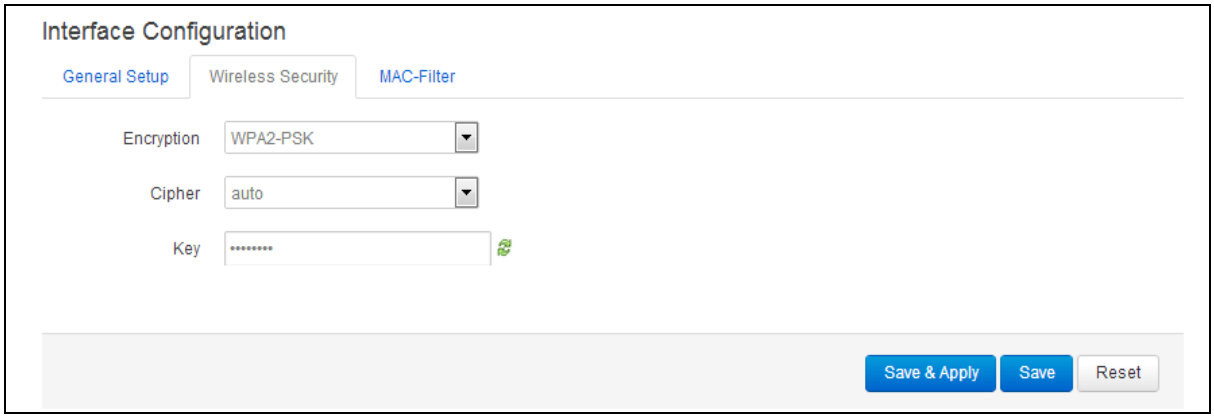


Figure 34: The wireless page interface configuration section

In the Encryption drop down menu, select the **encryption key**. When you have entered the encryption type, the Cipher and Key fields appear.

In the Cipher drop down menu, select the **cipher type**.

Create an encryption key.

Click **Save**.

In the top menu, select **Network -> Interfaces**. The Interfaces Overview page appears.

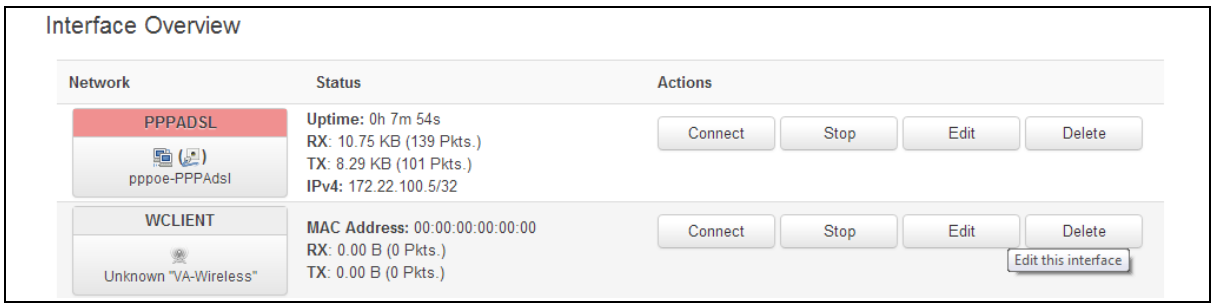


Figure 35: The interface overview page showing the newly created interface

Click **Edit** on the newly created interface. The Interfaces - WCLIENT page appears.

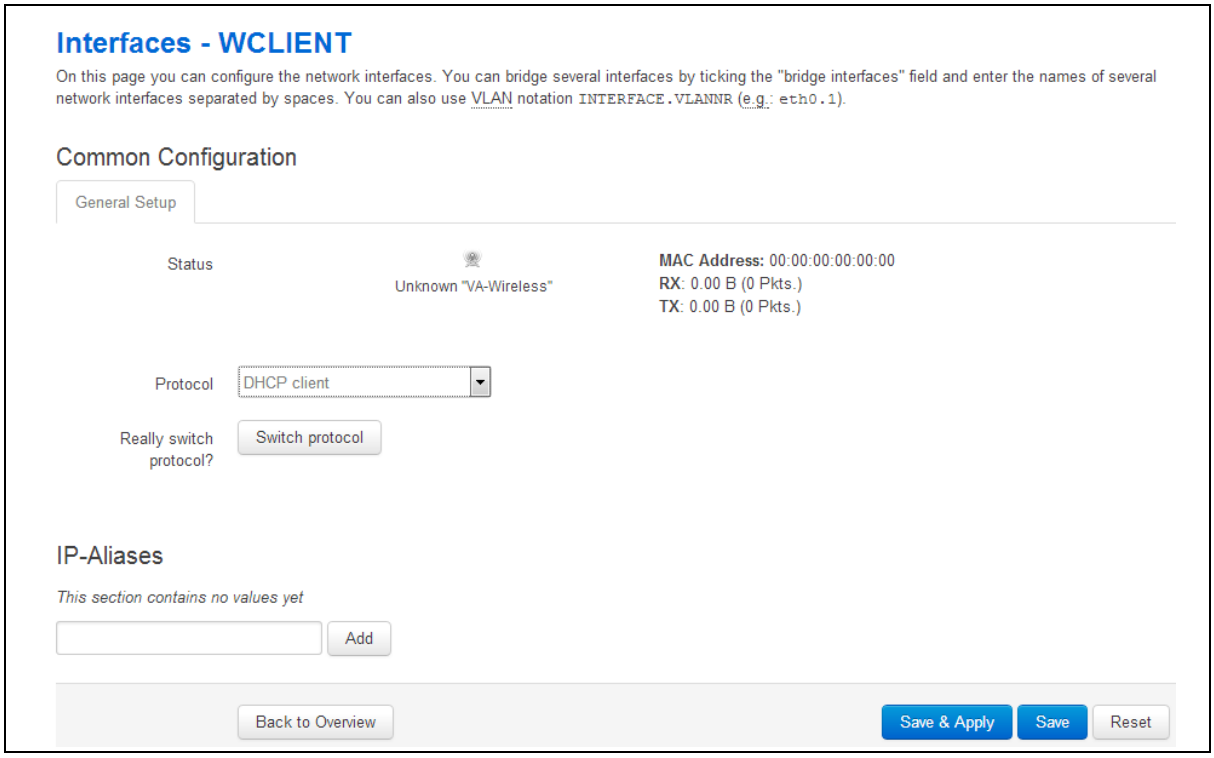

Interfaces - WCLIENT
On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).
Common Configuration
General Setup
Status
Unknown "VA-Wireless"
MAC Address: 00:00:00:00:00:00
RX: 0.00 B (0 Pkts.)
TX: 0.00 B (0 Pkts.)
Protocol
DHCP client
Really switch protocol?
Switch protocol
IP-Aliases
This section contains no values yet
Add
Back to Overview
Save & Apply
Save
Reset

Figure 36: The WClient interfaces page

In the Protocol drop down menu, select **DHCP client**. A 'Switch Protocol' button appears.

Click **Switch Protocol**.

Click **Save & Apply**.

Note: The router will now restart the network package. It may take up to one minute for connectivity to the router to be restored.

14.5 Configuring WiFi via UCI

14.5.1 Configuring Wi-Fi in AP mode on an existing Ethernet interface

The configuration files are stored on:

- Network file /etc/config/network
- Wireless file /etc/config/wireless

To view the configuration file, use the command:

uci export network

```
package network
config interface 'lan'
        option ifname 'eth0'
        option proto 'static'
        option ipaddr '192.168.100.1'
        option netmask '255.255.255.0'
        option type 'bridge'
```

or

uci export wireless

```
package wireless

config wifi-device 'radio0'
        option type 'mac80211'
        option channel '11'
        option phy 'phy0'
        option hwmode '11ng'
        option htmode 'HT20'
        list ht_capab 'SHORT-GI-40'
        list ht_capab 'TX-STBC'
        list ht_capab 'RX-STBC1'
        list ht_capab 'DSSS_CCK-40'
        option txpower '17'
        option country 'US'

config wifi-iface
        option device 'radio0'
        option mode 'ap'
        option disabled '1'
        option ssid 'Test_AP'
        option network 'lan'
        option encryption 'psk'
        option key 'secretkey'
```

To view UCI commands, enter:

uci show network

```
network.lan=interface
network.lan.ifname=eth0
network.lan.proto=static
network.lan.ipaddr=192.168.6.1
network.lan.netmask=255.255.255.0
network.lan.type=bridge
```

uci show wireless

```
wireless.radio0=wifi-device
wireless.radio0.type=mac80211
wireless.radio0.channel=11
wireless.radio0.phy=phy0
wireless.radio0.hwmode=11ng
wireless.radio0.htmode=HT20
wireless.radio0.ht_capab=SHORT-GI-40 TX-STBC RX-STBC1 DSSS_CCK-40
wireless.radio0.txpower=17
wireless.radio0.country=US
wireless.@wifi-iface[0]=wifi-iface
wireless.@wifi-iface[0].device=radio0
wireless.@wifi-iface[0].mode=ap
wireless.@wifi-iface[0].disabled=1
wireless.@wifi-iface[0].ssid=Test_AP
wireless.@wifi-iface[0].network=lan
wireless.@wifi-iface[0].encryption=psk
wireless.@wifi-iface[0].key=secretkey
```

14.5.2 Configuring WiFI on a new interface

uci export network

```
package network
config interface 'newlan'
        option proto 'static'
        option ipaddr '192.168.111.1'
        option netmask '255.255.255.0'
```

uci export wireless

```
package wireless

config wifi-device 'radio0'
        option type 'mac80211'
        option channel '11'
        option phy 'phy0'
        option hwmode '11ng'
        option htmode 'HT20'
        list ht_capab 'SHORT-GI-40'
        list ht_capab 'TX-STBC'
        list ht_capab 'RX-STBC1'
        list ht_capab 'DSSS_CCK-40'
        option txpower '17'
        option country 'US'

config wifi-iface
        option device 'radio0'
        option mode 'ap'
        option disabled '1'
        option ssid 'Test_AP'
        option network 'newlan'
        option encryption 'psk'
        option key 'secretkey'
```

To view UCI commands, enter:

uci show network

```
network.newlan=interface
network.newlan.proto=static
network.newlan.ipaddr=192.168.111.1
network.newlan.netmask=255.255.255.0
```

uci show wireless

```
wireless.radio0=wifi-device
wireless.radio0.type=mac80211
```

```
wireless.radio0.channel=11
wireless.radio0.phy=phy0
wireless.radio0.hwmode=11ng
wireless.radio0.htmode=HT20
wireless.radio0.ht_capab=SHORT-GI-40 TX-STBC RX-STBC1 DSSS_CCK-40
wireless.radio0.txpower=17
wireless.radio0.country=US
wireless.@wifi-iface[0]=wifi-iface
wireless.@wifi-iface[0].device=radio0
wireless.@wifi-iface[0].mode=ap
wireless.@wifi-iface[0].disabled=1
wireless.@wifi-iface[0].ssid=Test_AP
wireless.@wifi-iface[0].network=newlan
wireless.@wifi-iface[0].encryption=psk
wireless.@wifi-iface[0].key=secretkey
```

14.6 Configuring WiFi in client mode

uci export network

```
package network
config interface 'WCLIENT'
        option proto 'dhcp'
```

uci export wireless

```
package wireless

config wifi-device 'radio0'
        option type 'mac80211'
        option channel '11'
        option phy 'phy0'
        option hwmode '11ng'
        option htmode 'HT20'
        list ht_capab 'SHORT-GI-40'
        list ht_capab 'TX-STBC'
        list ht_capab 'RX-STBC1'
        list ht_capab 'DSSS_CCK-40'
```

```
        option txpower '17'
        option country 'US'

config wifi-iface
        option device 'radio0'
        option ssid 'Remote-AP'
        option mode 'sta'
        option network 'WCLIENT'
        option encryption 'psk2'
        option key 'testtest'
```

To view UCI commands, enter:

uci show network

```
network.WCLIENT=interface
network.WCLIENT.proto=dhcp
```

uci show wireless

```
wireless.radio0=wifi-device
wireless.radio0.type=mac80211
wireless.radio0.channel=11
wireless.radio0.phy=phy0

wireless.radio0.hwmode=11ng
wireless.radio0.htmode=HT20
wireless.radio0.ht_capab=SHORT-GI-40 TX-STBC RX-STBC1 DSSS_CCK-40
wireless.radio0.txpower=17
wireless.radio0.country=US
wireless.@wifi-iface[0]=wifi-iface
wireless.@wifi-iface[0].device=radio0
wireless.@wifi-iface[0].ssid=Remote-AP
wireless.@wifi-iface[0].mode=sta
wireless.@wifi-iface[0].network=WCLIENT
wireless.@wifi-iface[0].encryption=psk2
wireless.@wifi-iface[0].key=testtest
```

15 Configuring a 3G/4G connection

In the top menu, select **Network -> Interfaces**.

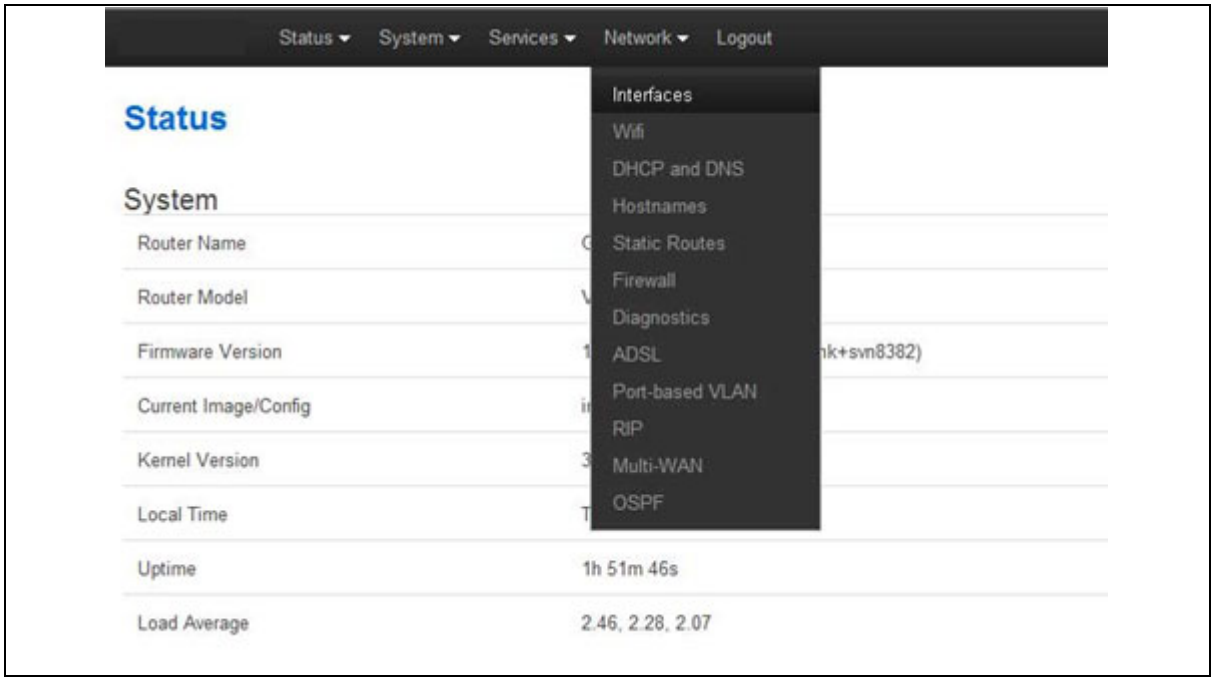


Figure 37: The interfaces menu on a VA router

The Interfaces Overview page appears.

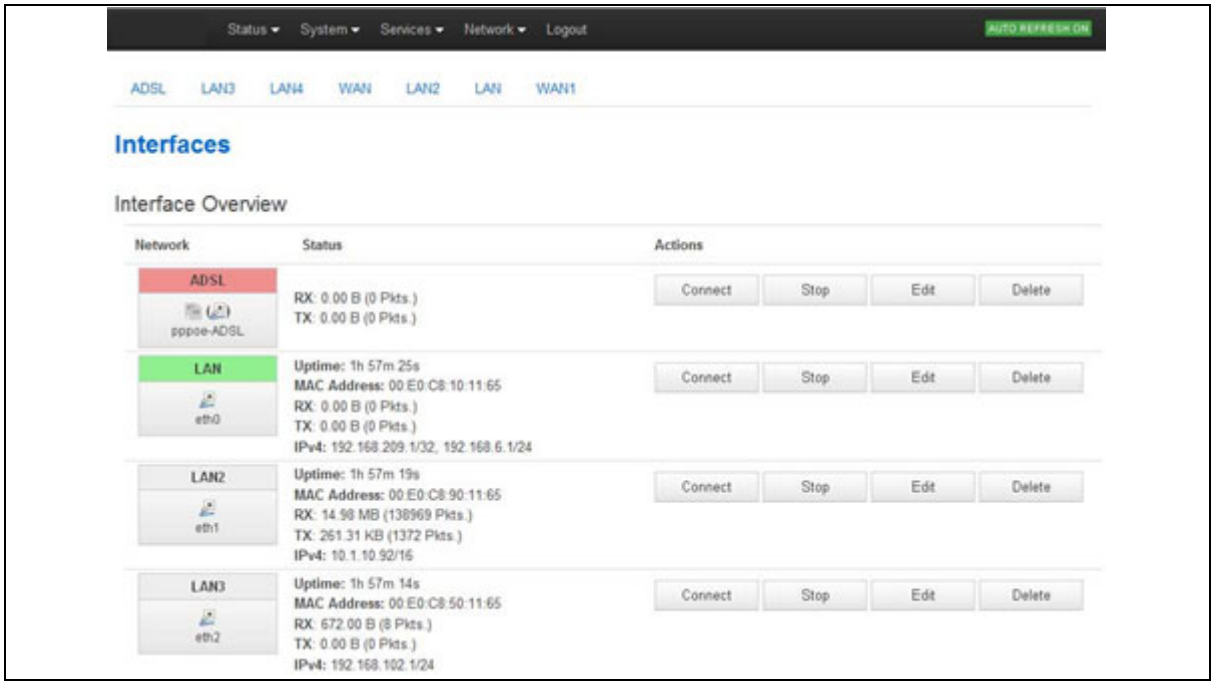


Figure 38: The interfaces overview page.

Click **Edit** on WAN or LAN to make your changes.

For WAN connectivity, the Common Configuration page appears.

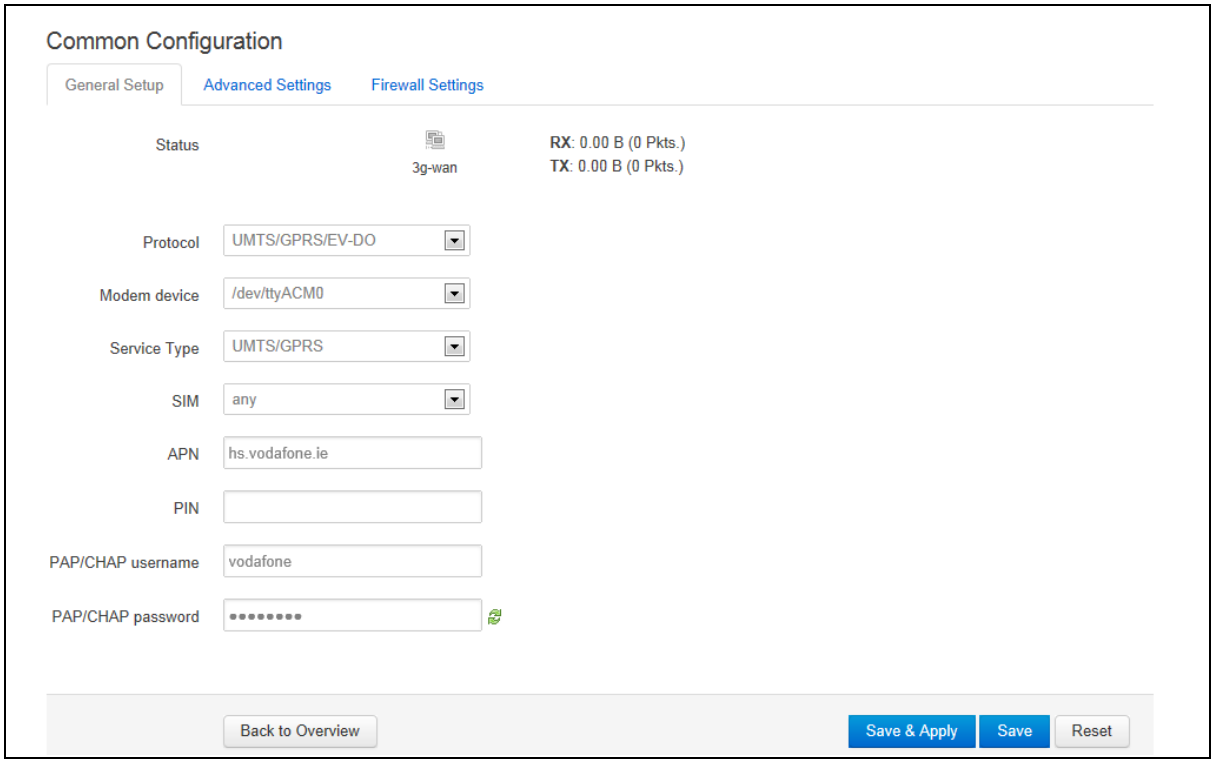


Figure 39: The common connectivity page

Ensure the General Setup tab is selected.

For single SIM implementation, in the SIM drop down menu, select **SIM 1**.

Enter the APN information and the PAP/CHAP username and password.

Click **Save & Apply**.

To enable 3G/4G connection to connect on boot up, select the **Advanced Settings** tab.

Select **Bring up on boot**.

Click **Save & Apply**.

To check for connectivity, return to the top menu, and under **Network -> Interfaces**, the WAN interface will show receive and transmit packets and an IP address.

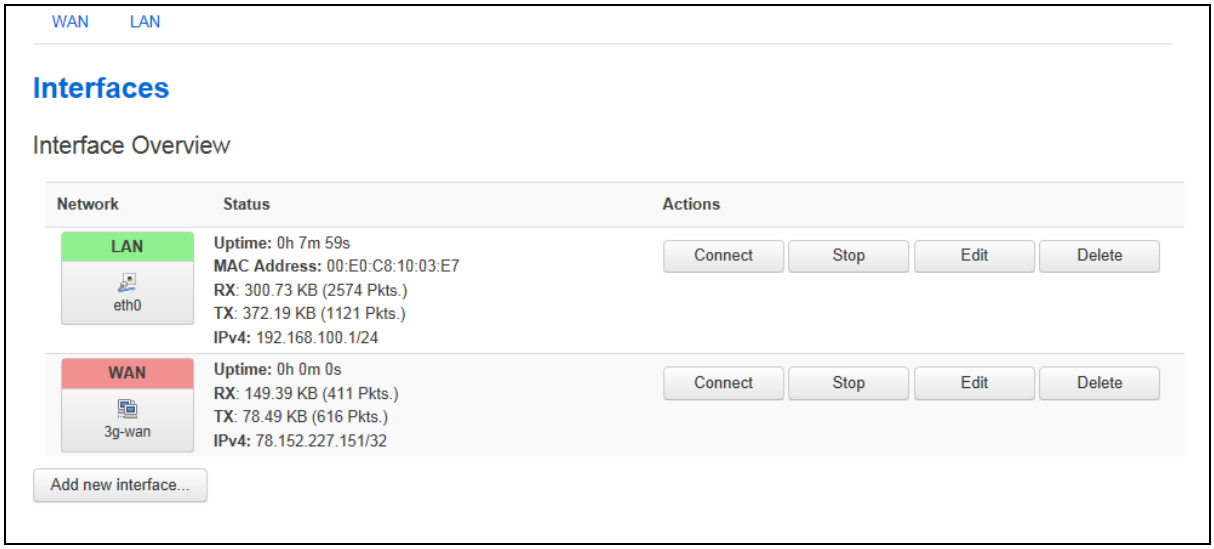


Figure 40: The interfaces overview page

To view 3G/4G connectivity information, browse to **Status -> 3G Stats**.

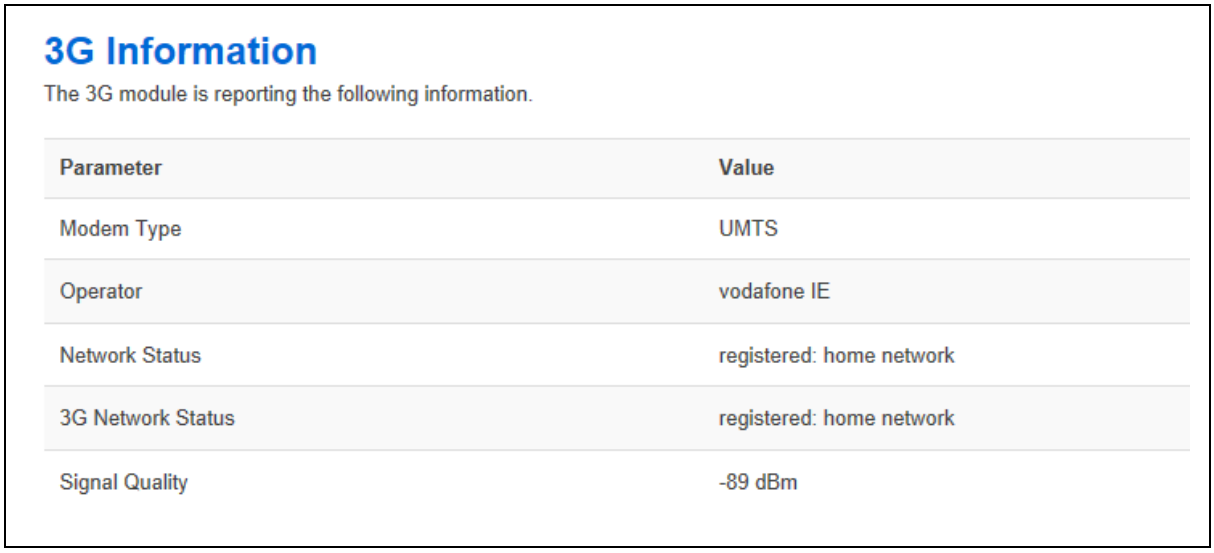


Figure 41: The 3G information page

16 Configuring SMS

Browse to the router's IP address and login.

Select **Service tab > Mobile Manager**. The Mobile Manager page appears.

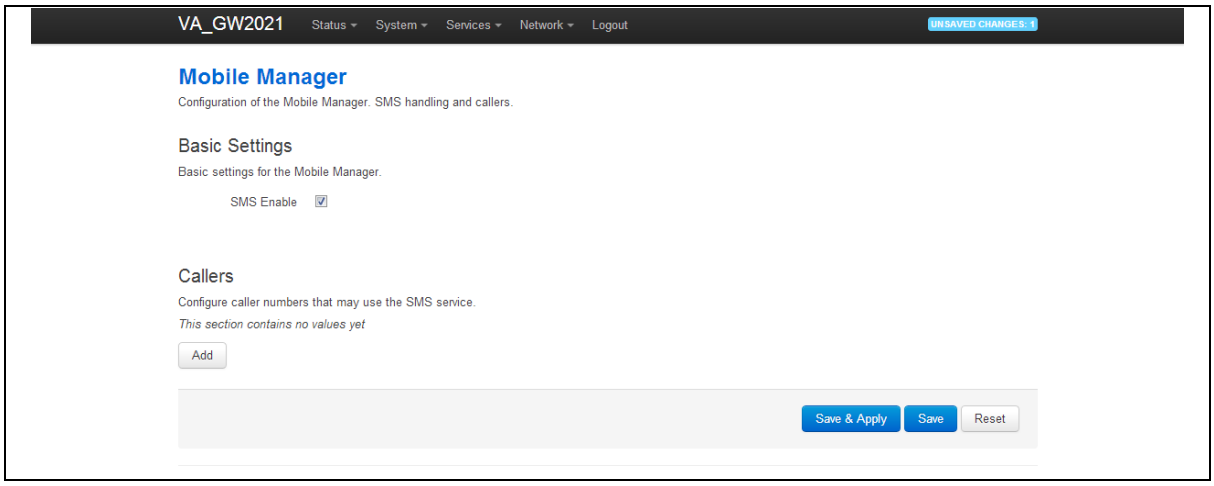
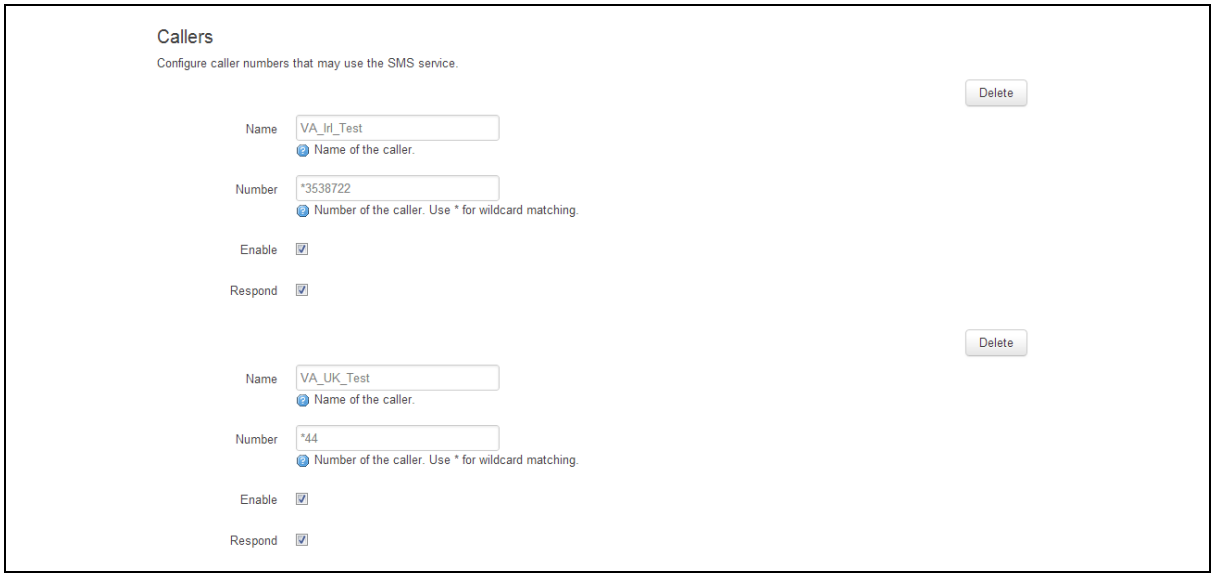


Figure 42: The mobile manager page

In the Basic Settings section, check the box beside **SMS Enable**.

In the Callers section, click **Add** to add caller numbers.

Add in specific caller numbers or use the wildcard symbol * as shown below.



Click **Enable**.

Select **Respond** if you want the router to reply.

Parameter	Description
Name	Name assigned to caller.
Number	Number of caller allowed to SMS the router.
Enable	Enables or disables caller.
Respond	If checked, the router will return an SMS.

Table 7: Scripting commands and their descriptions

When you have made your changes, click **Save & Apply** and then reboot.

16.1 Monitoring SMS

You can monitor inbound SMS messages using the router's web browser or via an SSH session.

To monitor via SSH, login and enter `logread –f&`. An outgoing SMS message appears.

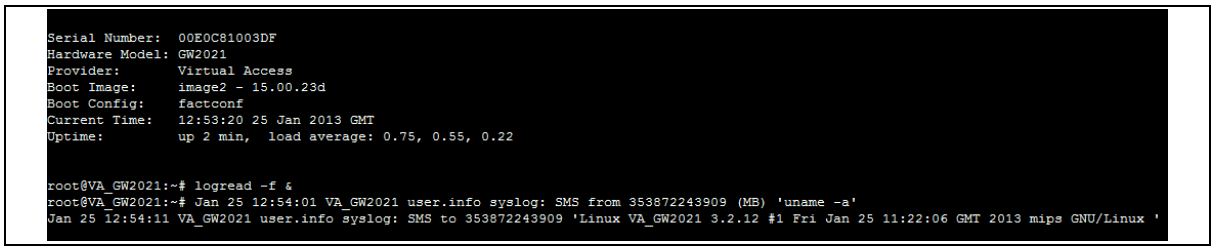

Serial Number: 00E0C81003DF
Hardware Model: GW2021
Provider: Virtual Access
Boot Image: image2 - 15.00.23d
Boot Config: factconf
Current Time: 12:53:20 25 Jan 2013 GMT
Uptime: up 2 min, load average: 0.75, 0.55, 0.22
root@VA_GW2021:~# logread -f &
root@VA_GW2021:~# Jan 25 12:54:01 VA_GW2021 user.info syslog: SMS from 353872243909 (MB) 'uname -a'
Jan 25 12:54:11 VA_GW2021 user.info syslog: SMS to 353872243909 'Linux VA_GW2021 3.2.12 #1 Fri Jan 25 11:22:06 GMT 2013 mips GNU/Linux '

Figure 43: Output from the command logread –f&

To monitor via the web browser, login and select **Status >system log**.

Scroll to the bottom of the log to view the SMS message.

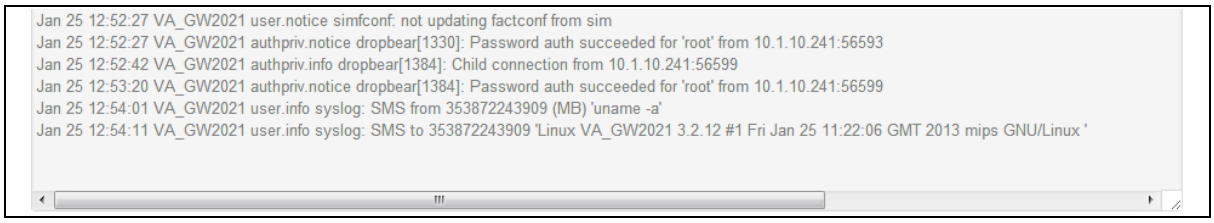

Jan 25 12:52:27 VA_GW2021 user.notice simfconf: not updating factconf from sim
Jan 25 12:52:27 VA_GW2021 authpriv.notice dropbear[1330]: Password auth succeeded for 'root' from 10.1.10.241:56593
Jan 25 12:52:42 VA_GW2021 authpriv.info dropbear[1384]: Child connection from 10.1.10.241:56599
Jan 25 12:53:20 VA_GW2021 authpriv.notice dropbear[1384]: Password auth succeeded for 'root' from 10.1.10.241:56599
Jan 25 12:54:01 VA_GW2021 user.info syslog: SMS from 353872243909 (MB) 'uname -a'
Jan 25 12:54:11 VA_GW2021 user.info syslog: SMS to 353872243909 'Linux VA_GW2021 3.2.12 #1 Fri Jan 25 11:22:06 GMT 2013 mips GNU/Linux '

Figure 44: Output from system log

16.2 Outgoing messages

You can send an outgoing message via the command line using the following syntax.

```
sendsms 353872243909 ‘hello’
```

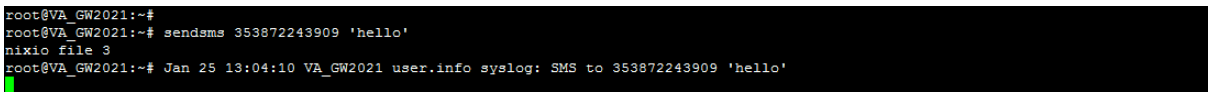

root@VA_GW2021:~#
root@VA_GW2021:~# sendsms 353872243909 'hello'
nixio file 3
root@VA_GW2021:~# Jan 25 13:04:10 VA_GW2021 user.info syslog: SMS to 353872243909 'hello'

Figure 45: Output from the syntax sendsms 353872243909 ‘hello

17 Configuring Multi-WAN

Multi-WAN is used for managing WAN interfaces on the router, for example, 3G interfaces to ensure high-availability. You can customise Multi-WAN to various needs, but its main use is to ensure WAN connectivity and provide a failover system in the event of failure or poor coverage.

17.1 Multi-WAN web interface

You can configure Multi-WAN through the web interface. In the navigation menu browse to **Network -> Multi-Wan**. The Multi-WAN page appears.

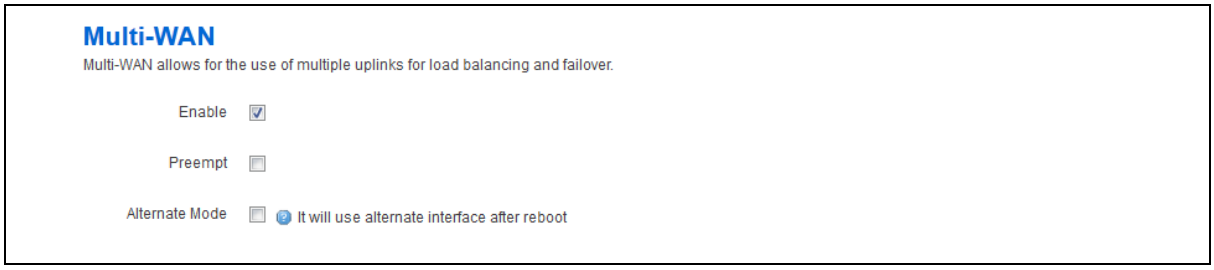

Multi-WAN
Multi-WAN allows for the use of multiple uplinks for load balancing and failover.
Enable
Preempt
Alternate Mode
It will use alternate interface after reboot

Figure 46: The multi-WAN page

Name	Type	Required	Default	Description
Enable	Boolean	Yes	No	Enables or disables Multi-WAN.
Preempt	Boolean	No	No	Enables or disables pre-emption for Multi-WAN. If enables the router will keep trying to connect to a higher priority interface depending on timer set.
Alternate Mode	Boolean	No	No	Enables or disables alternate mode for Multi-WAN. If enabled the router will use an alternate interface after reboot.

Table 8: The multi-WAN fields and their descriptions

When you have enabled Multi-WAN, you can add the interfaces that will be managed by Multi-WAN, for example 3G interfaces.

Note: the name used for multi-WAN must be identical, including upper and lowercases, to the actual 3G interface name defined in your network configuration. To check the names and settings are correct, browse to **Network - > interfaces** or alternatively, run: **cat / etc / config / network** through CLI.

Enter the name of the WAN interface to configure, and then click **Add**. The new section for configuring specific parameters will appear.

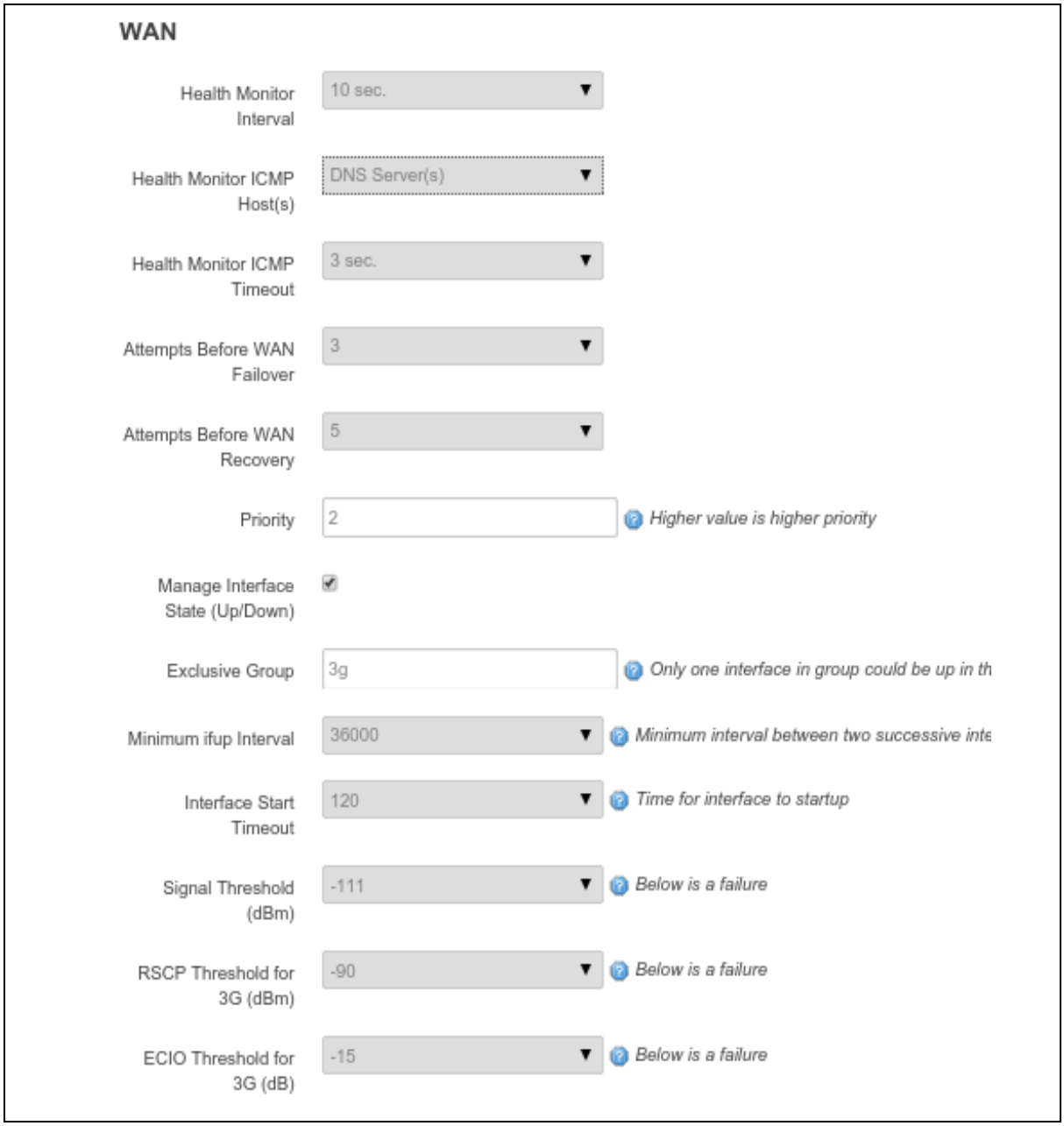


Figure 47: Example interface showing failover traffic destination as the added multi-WAN interface

Name	Type	Required	Default	Description
Load Balancer Distribution	Dropdown list	No	10	Configures weight for load-balancing. It is not applicable if you are using 2 SIM cards.
Health Monitor Interval	Dropdown list	No	10	Sets the period to check health status of interface.
Health Monitor ICMP Host(s)	Dropdown list/IP address	No	DNS Server(s)	Sends Health ICMPs to configured value DNS servers by default. Configure to any address.
Health Monitor ICMP Timeout	Dropdown list	No	3 secs	Sets Ping timeout in seconds.

Attempts Before WAN Failover	Dropdown list	No	3	Sets the amount of retries before interface is considered a failure.
Attempts Before WAN Recovery	Dropdown list	Yes	5	Sets the number of healthy pings before the interface is considered healthy.
Failover Traffic Destination	Dropdown list	Yes	Load Balancer (Compatibility)	This field is not applicable unless you have 2 WAN interfaces connected simultaneously and want to forward traffic to a specific interface after the failover.
DNS Server(s)	Dropdown list	No	Auto	Specifies DNS for the interface.
Priority	Numeric value	Yes	0	Specifies the priority of the interface, a higher value is better. 1 is better than 0, therefore the interface with priority of 1 will connect first.
Manage Interface State (Up/Down)	Boolean	Yes	Yes	Sets the interface start/stop by Multi-WAN.
Exclusive Group	Numeric value	No	0	Defines the interface within the group, only one interface can be active: SIM 1 or SIM 2.
Minimum ifup interval	Dropdown list/Numeric value	Yes	300 secs	Specifies the time for interface to start up. If it is not up after this period, it will be considered a fail.
Interface Start Timeout	Dropdown list/Numeric value	Yes	40 secs	Specifies the minimum interval between two successive interface start attempts.
Signal Threshold (dBm)	Dropdown list/Numeric value	Yes	-150	Specifies the minimum dBm signal strength before considering if the interface fails signal health check.
RSCP Threshold (dBm)	Dropdown list/Numeric value	Yes	-150	Specifies the minimum RSCP signal strength before considering if the interface fails signal health check.
ECIO Threshold (dBm)	Dropdown list/Numeric value	Yes	-35	Specifies the minimum ECIO signal strength before considering if the interface fails signal health check.

Table 9: Multi-WAN interface fields and their descriptions

You can also set up traffic rules, to forward specific traffic out of the right WAN interface, based on source, destination address, protocol or port. This is useful to force traffic on specific interfaces when using multiple WAN interfaces simultaneously.

Figure 48: The multi-WAN traffic rules page

17.2 Multi-WAN UCI interface

Multi-WAN UCI configuration settings are stored in the following file:

/etc/config/multiwan

Run UCI export or show commands to see Multi-WAN UCI configuration settings. A sample is shown below.

```
~# uci export multiwan
package multiwan

config multiwan 'config'
        option preempt 'yes'
        option alt_mode 'no'
        option enabled 'yes'

config interface 'wan'
        option disabled '0'
        option health_interval '10'
        option timeout '3'
        option health_fail_retries '3'
        option health_recovery_retries '5'
        option priority '2'
        option manage_state 'yes'
        option exclusive_group '3g'
        option ifup_retry_sec '36000'
        option icmp_hosts 'disable'
        option signal_threshold '-111'
        option rscp_threshold '-90'
```

```
        option ecio_threshold '-15'
        option ifup_timeout_sec '120'

~# uci show multiwan
multiwan.config=multiwan
multiwan.config.preempt=yes
multiwan.config.alt_mode=no
multiwan.config.enabled=yes
multiwan.wan=interface
multiwan.wan.disabled=0
multiwan.wan.health_interval=10
multiwan.wan.timeout=3
multiwan.wan.health_fail_retries=3
multiwan.wan.health_recovery_retries=5
multiwan.wan.priority=2
multiwan.wan.manage_state=yes
multiwan.wan.exclusive_group=3g
multiwan.wan.ifup_retry_sec=36000
multiwan.wan.icmp_hosts=disable
multiwan.wan.signal_threshold=-111
multiwan.wan.rscp_threshold=-90
multiwan.wan.ecio_threshold=-15
```

Config multiwan

Name	Required	Default	Description
Enabled	Yes	No	Enables or disables Multi-WAN.
Preempt	No	No	Enables or disables pre-emption for Multi-WAN. If enabled, the router will keep trying to connect to a higher priority interface depending on timer set.
alt mode	No	No	Enables or disables alternate mode for Multi-WAN. If enabled the router will use an alternate interface after reboot.

Config interface

Name	Required	Default	Description
Disabled	No	0	Disables the Multi-WAN interface.
Weight	No	10	Configures weight for load-balancing. Not relevant when two SIM cards are being used.
Health interval	No	10	Sets the period to check health status of interface.

Icmp hosts	No	3 secs	Sets Ping timeout.
timeout	No	3 secs	Sets Ping timeout.
Health fail retries	Yes	3	Specifies the amount of retries before the interface is considered a failure.
Health recovery retries	Yes	5	Specifies the number of healthy pings before the interface is considered healthy.
failover to	Yes	Load Balancer (Compatibility)	This field is not applicable unless you have two WAN interfaces connected simultaneously and want to forward traffic to a specific interface after the failover.
dns	No	Auto	Defines DNS for the interface.
priority	Yes	0	Specifies the priority of the interface, a higher value is better. 1 is better than 0, therefore the interface with priority of 1 will connect first.
manage state	Yes	Yes	Specifies interface start/stop by Multi-WAN.
exclusive group	No	0	Specifies which interface within the group is active. Only one interface can be active: SIM 1 or SIM 2.
ifup retry sec	Yes	300 secs	Specifies the time for interface to start up. If it is not up after this period, it will be considered a fail.
ifup timeout sec	Yes	40 secs	Specifies the minimum interval between two successive interface start attempts.
signal threshold	Yes	-150	Specifies the minimum dBm signal strength before considering the interface as fail.
RSCP Threshold for 3G (dBm)	Yes	-150	Specifies the minimum RSCP signal strength before considering the interface as fail.
ECIO Threshold for 3G (dBm)	Yes	-35	Specifies the minimum ECIO signal strength before considering the interface as fail.

18 Automatic operator selection

18.1 Introduction to automatic operator selection

This section describes how to configure and operate the Automatic Operator Selection feature of a Virtual Access router.

When the roaming SIM is connected, the 3G module has the ability to scan available 3G networks. The router, using mobile and multi-WAN packages, finds available networks to create and sort interfaces according to their signal strength. These interfaces are used for failover purposes.

18.2 Configuring automatic operator selection

While the router boots up it checks for 3G networks. Based on available networks, the router creates network and multi-WAN package failover interfaces. Details for these interfaces are provided in the mobile package. When you have created the interfaces, multi-WAN manages the operation of primary (predefined) and failover (auto created) interfaces.

There are four PMP (Primary Mobile Provider) scenarios:

- PMP + roaming: pre-empt enabled
- PMP + roaming: pre-empt disabled
- No PMP + roaming
- Disable roaming

18.3 Configuring automatic operator selection via the web interface

18.3.1 PMP + roaming: pre-empt enabled

In this scenario, the primary interface is used whenever possible.

Software operations

1. Connect the PMP interface.
2. Wait until the signal level on the PMP interface goes under sig_dbm option value.
3. Disconnect the PMP interface.
4. Connect the first auto-generated interface.
5. Wait until the signal level on the first auto-generated interface goes under the sig_dbm option in the mobile package, or until the primary interface is available to connect after it was disconnected in step 3. ifup_retry_sec option value of primary interface in multi-WAN package.
6. Disconnect auto-generated interface. If the interface was disconnected due to low signal level then connect the next auto-generated interface and repeat step 5. If the

interface was disconnected because ifup_retry_sec of Primary interface timed out then go back to step 1 and repeat the process.

The primary predefined interface is defined in the network package. Ensure the interface name matches the interface name defined in the multi-WAN package.

18.3.1.1 Creating primary predefined interface

On the web interface go to **Network ->Interfaces**. The Interfaces page appears.

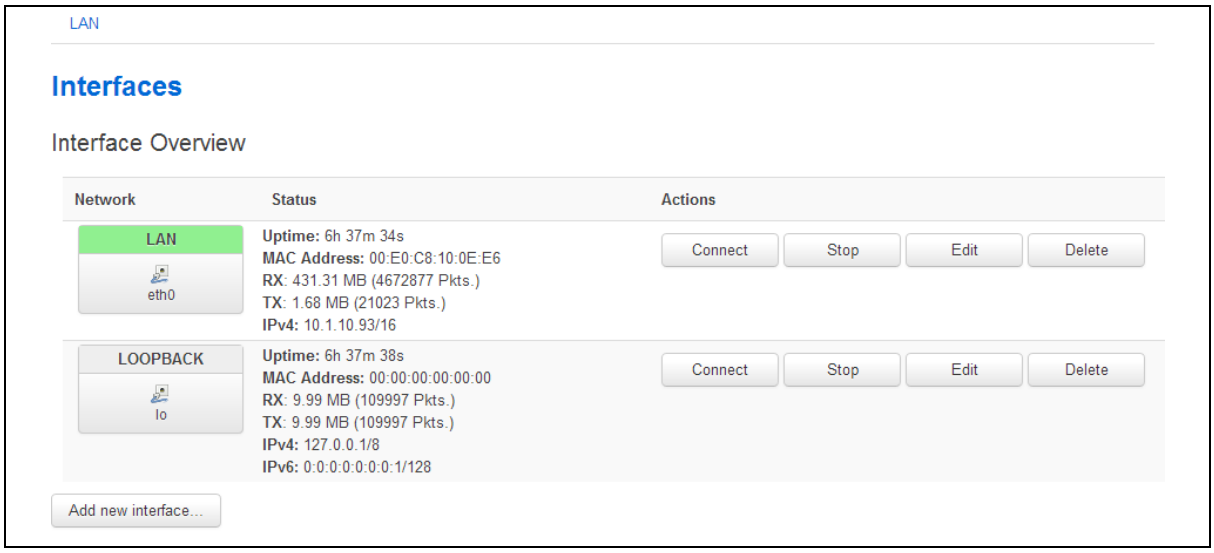


Figure 49: The interface overview page

Click **Add new interface...** The Create Interface page appears.

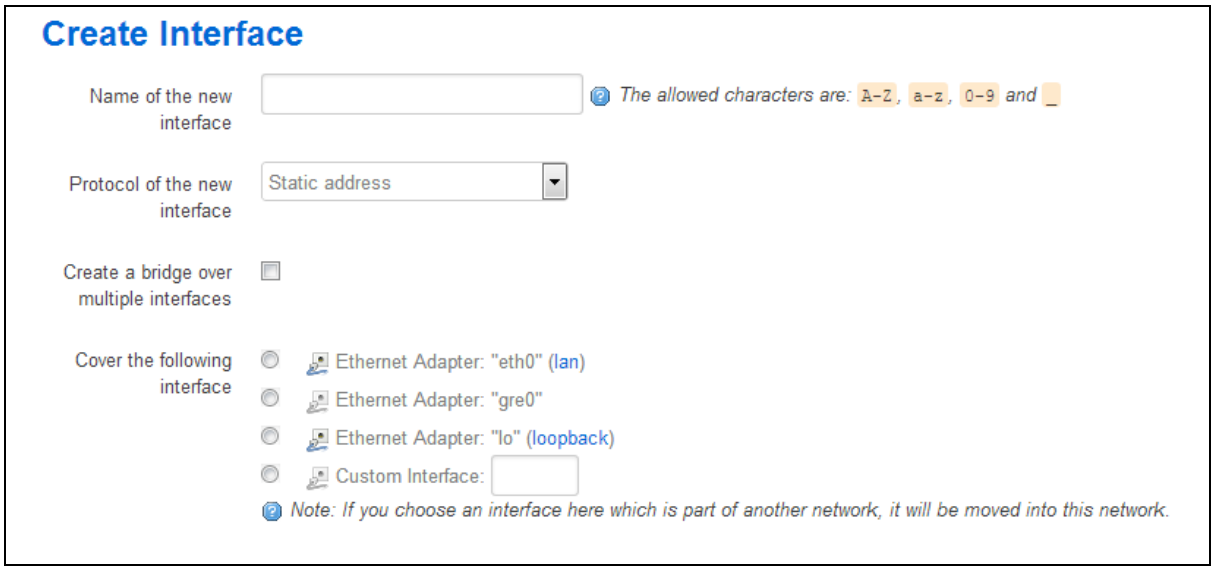

Create Interface
Name of the new interface
The allowed characters are: A-Z, a-z, 0-9 and _
Protocol of the new interface
Static address
Create a bridge over multiple interfaces
Cover the following interface
Ethernet Adapter: "eth0" (lan)
Ethernet Adapter: "gre0"
Ethernet Adapter: "lo" (loopback)
Custom Interface:
Note: If you choose an interface here which is part of another network, it will be moved into this network.

Figure 50: The create interface page

Type in the name of the interface in Name of the new interface field.

Type the Interface Name in following format: **3g_s<sim-number>_<short-operator-name>**. Where <sim-number> is number of roaming SIM (1 or 2)

and <short-operator-name> is first four alphanumeric characters of operator name (as reported by 'AT+COPS=?' command).

Type the short operator name in lower case, for example:

Operator name	First four alphanumeric numbers
Vodafone UK	voda
O2 – UK	o2uk
Orange	oran

Table 10: Examples of operator names

From the Protocol dropdown menu, select UMTS/GPRS/EV-DO.

Click **Submit**. The Common Configuration page appears

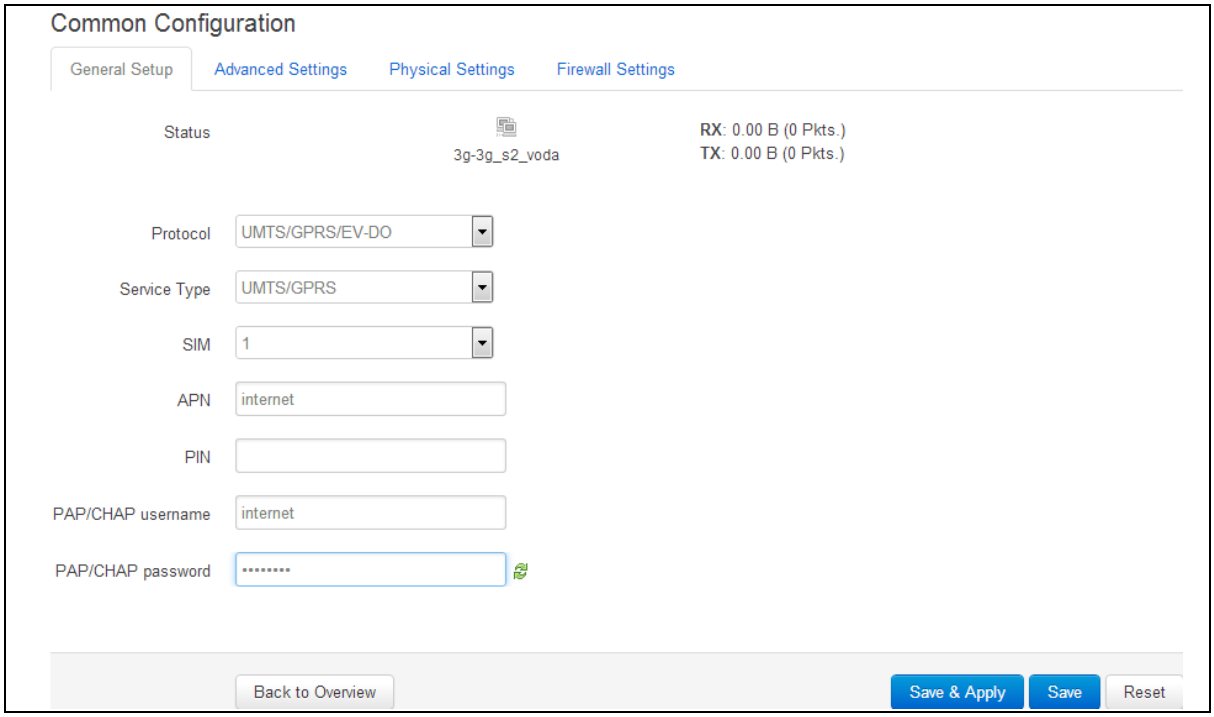


Figure 51: The common configuration page

Name	Type	Required	Default	Description
Protocol	Dropdown menu	Yes	UMTS/GPRS/EV-DO	Protocol type
Service Type	Dropdown menu	Yes	None	Service type that will be used to connect to the network
SIM	Dropdown menu	Yes	None	APN name of Mobile Network Operator
PIN	Numeric value	No	None	SIM Card's PIN number
PAP/CHAP username	String	No	None	Username used to connect to APN
PAP/CHAP password	String	No	None	Password used to connect to APN

Click **Save & Apply**.

18.3.1.2 Setting multi-WAN options for primary predefined interface

On the web interface go to **Network ->Multi-Wan**. The Multi-WAN page appears.

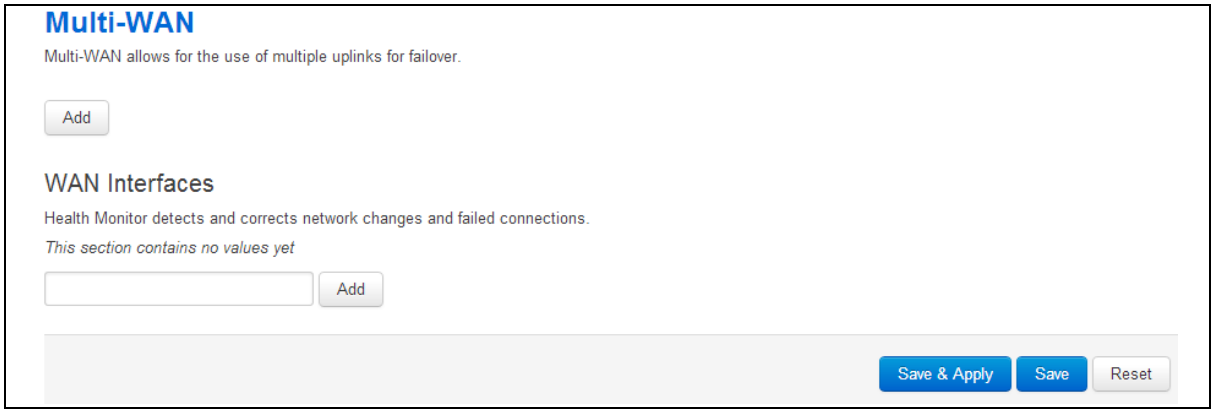


Figure 52: The multi-WAN page

In the Multi-WAN page, click **Add**. The Multi-WAN page appears.

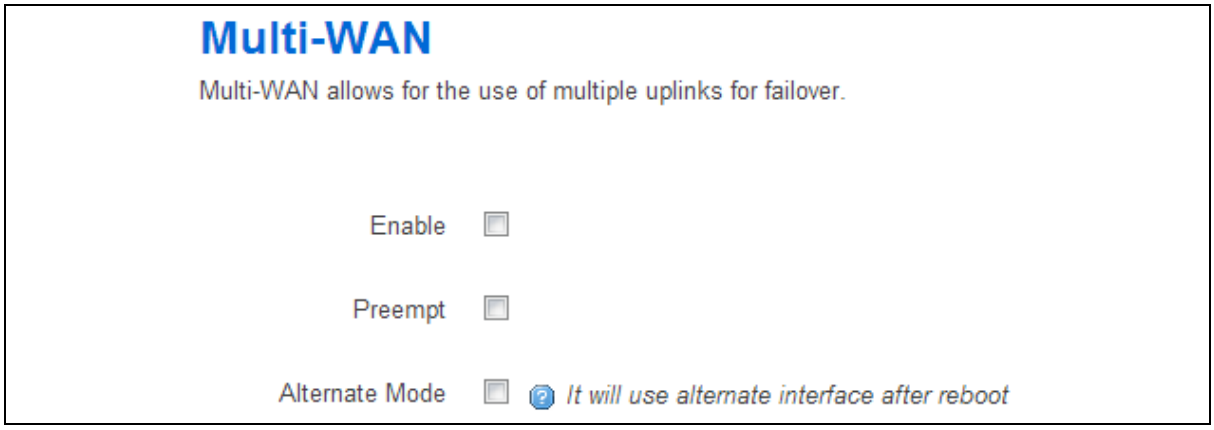


Figure 53: The multi-wan page

Check **Enable**.

Check **Preempt**.

Name	Type	Required	Default	Description
Enable	Boolean	Yes	0	Enables Multi-Wan
Preempt	Boolean	No	0	Enables Preempt mode
Alternate Mode	Boolean	No	0	Enables Alternate Mode

In the WAN Interfaces section, type in the name of the Multi-WAN Interface.

Note: this name should match the name specified in the previous section.

Click **Add**. The Multi-WAN page appears.

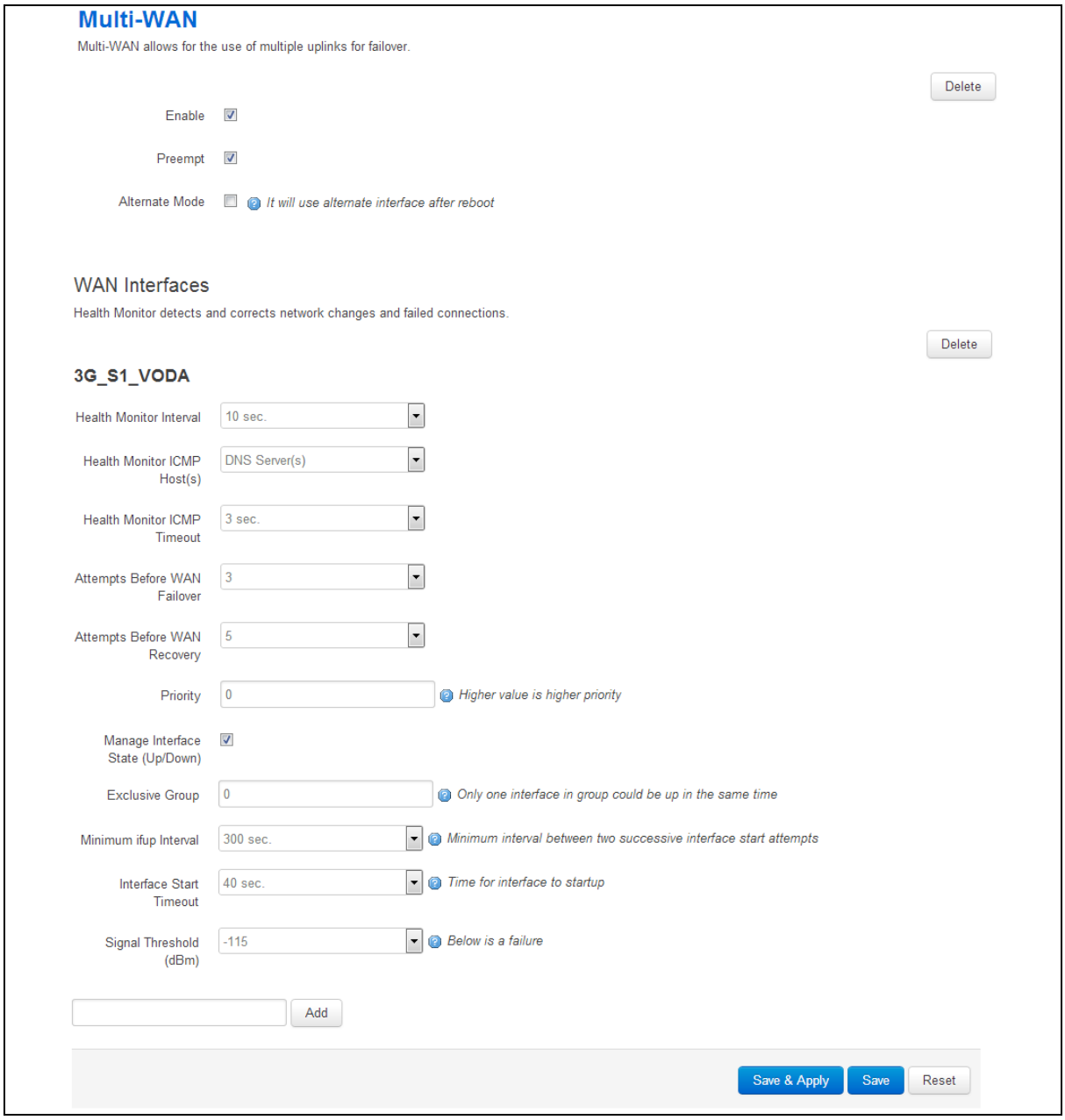


Figure 54: The multi-WAN page

From the Health Monitor Interval dropdown menu, choose the interval that will be used to monitor signal strength value.

From the Attempts Before WAN Failover dropdown menu, select the number of fail attempts of Health Monitor checks that will cause the interface to be disconnected.

In the Priority field, type in the priority number. The Multi-Wan interface priority must be higher than one specified in package mobile 'Setting options for Automatically Created interfaces' section below.

Ensure you have selected the Manage Interface State (Up/Down) option.

In the Exclusive Group field type in **3g**.

From the dropdown menu, select the **Choose Minimum ifup Interva**l option.

From dropdown menu, select the **Interface Start Timeout** option.

From dropdown menu, select the **Signal Threshold** option.

All available WAN interface options are described in the table below.

Name	Type	Required	Default	Description
Health Monitor Interval	Dropdown menu	Yes	10 sec	Interval used to monitor Signal strength
Health Monitor ICMP Host(s)	Dropdown menu	No	none	Target IP address for ICMCP packets
Health Monitor ICMP Timeout	Dropdown menu	Yes	3 sec	ICMP timeout
Attempts Before WAN Failover	Dropdown menu	Yes	3	Number of fail attempts of Health Monitor before interface is torn down
Attempts Before WAN Recovery	N/A	N/A	N/A	N/A
Priority	Number	Yes	0	Higher value is higher priority
Minimum ifup Interval	Dropdown menu	Yes	300 sec	Minimum interval between two successive interface start attempts
Interface Start Timeout	Dropdown menu	Yes	40 sec	Time for interface to startup
Signal Threshold (dBm)	Dropdown menu	Yes	-115	if signal is lower than this then is marked as fail

18.3.1.3 Setting options for automatically created interfaces

From the top menu on the web interface page, select **Services -> Mobile Manager**. The Mobile Manager page appears.

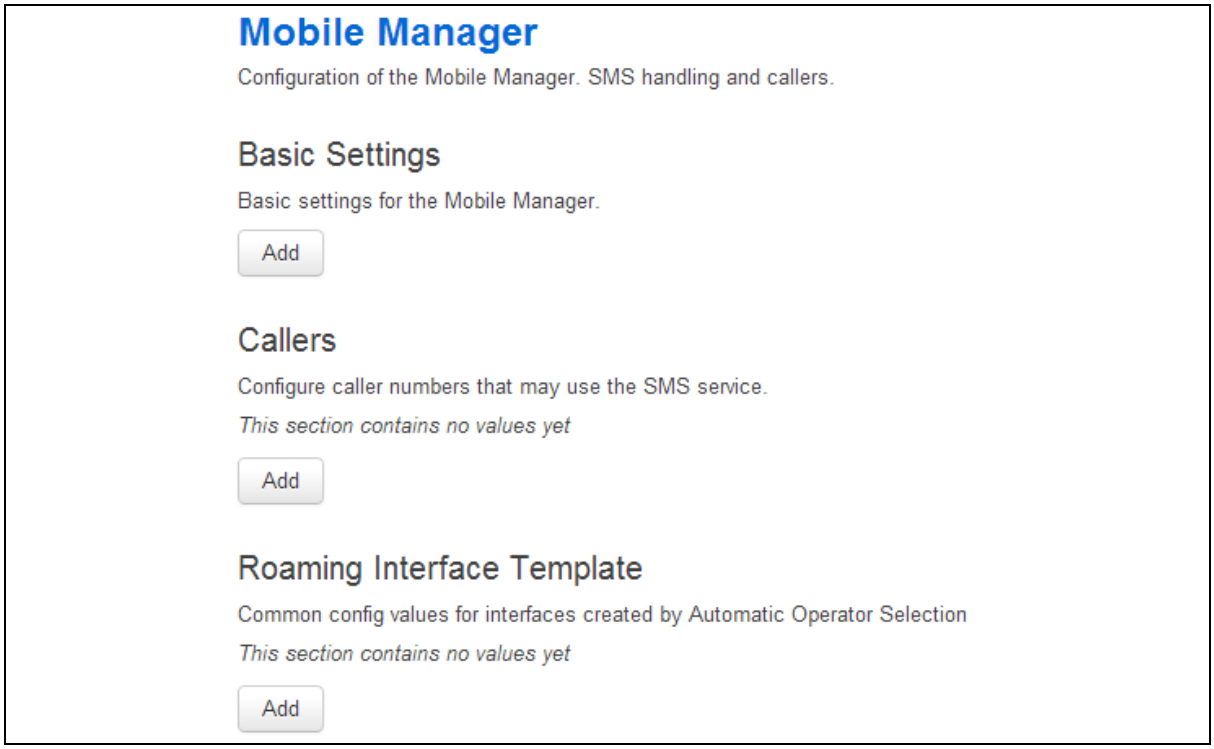

Mobile Manager
Configuration of the Mobile Manager. SMS handling and callers.
Basic Settings
Basic settings for the Mobile Manager.
Add
Callers
Configure caller numbers that may use the SMS service.
This section contains no values yet
Add
Roaming Interface Template
Common config values for interfaces created by Automatic Operator Selection
This section contains no values yet
Add

Figure 55: The mobile manager page

Under Basic Settings, click **Add**. The Basic settings for Mobile Manager page appears.

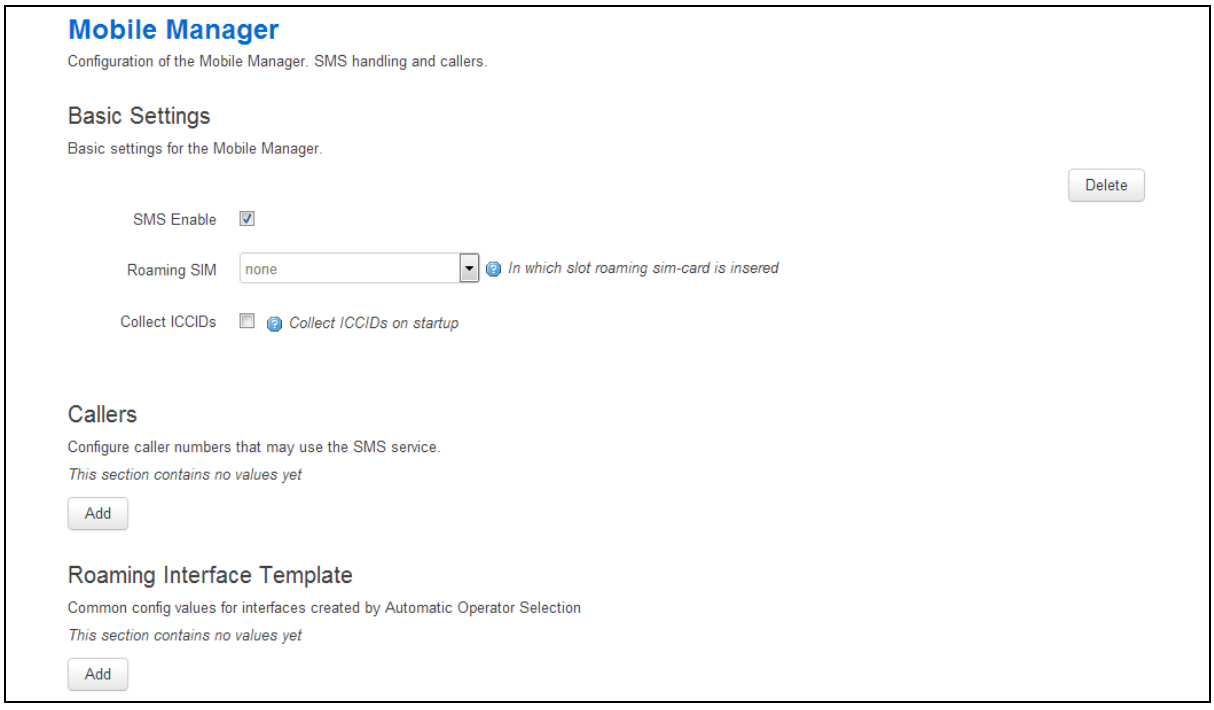


Figure 56: Basic settings field in the mobile manager page

Name	Type	Required	Default	Description
SMS Enable	Boolean	No	1	Enables SMS
Roaming SIM	Dropdown list	Yes	none	In which slot roaming sim-card is inserted
Collect ICCIDs	Boolean	No	0	Collect ICCIDs on startup from one (when 0) or from two SIMs (1)

Under Roaming Template Interface click **Add**. The Roaming Interface Template page appears.

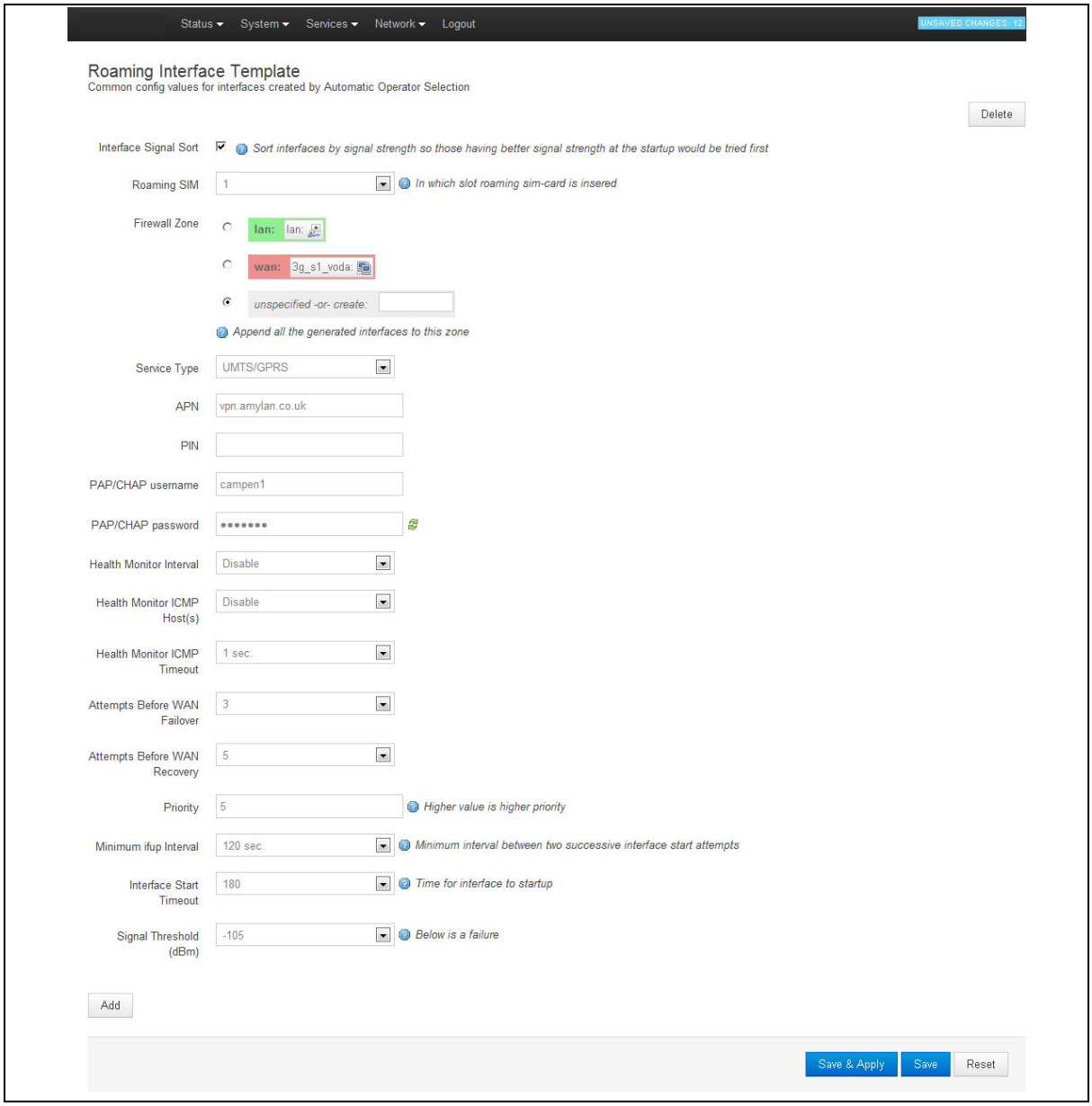


Figure 57: The roaming interface template page

Check the Interface Signal Sort checkbox, so auto created interfaces are sorted in priority, based on signal strength value.

From the Roaming SIM dropdown menu, select the slot that the roaming SIM card should be inserted in to.

Click the **Firewall zone** radio button to select the zone that the auto created interface will belong to.

Type in the CHAP **username** and **password**.

Type in **APN** and **PIN** details.

From the Health Monitor Interval dropdown menu, select the interval that will be used to monitor signal strength value.

From the Attempts Before WAN Failover dropdown menu, select the number of fail attempts of Health Monitor checks that will cause the interface to be disconnected.

From the Minimum ifup Interval dropdown menu, select the minimum interval between two successive interface start attempts.

From the Interface Start Timeout dropdown menu, select the time for the interface to start up.

From the Choose Signal Threshold dropdown menu, select the fail number point.

Name	Type	Required	Default	Description
Interface Signal Sort	Boolean	No	0	Sorts interfaces by signal strength so those having better signal strength at the startup will be tried first
Roaming SIM	Dropdown menu		1	Specifies which slot roaming SIM-card is inserted.
Firewall Zone	Radio button menu	No	None	Adds all generated interfaces to this zone.
Service Type	Dropdown menu	Yes	UMTS/GPRS	Specifies technology type.
APN	String	Yes	None	Sets APN settings.
PIN	Number	No	None	Sets SIM card PIN number.
PAP/CHAP username	String	No	None	Sets username used to connect to APN.
PAP/CHAP password	String	No	None	Sets password used to connect

				to APN.
Health Monitor Interval	Dropdown menu	Yes	10 sec	Sets interval used to monitor signal strength.
Health Monitor ICMP Host(s)	Dropdown menu	No	none	Specifies target IP address for ICMCP packets.
Health Monitor ICMP Timeout	Dropdown menu	Yes	3 sec	Specifies ICMP timeout.
Attempts Before WAN Failover	Dropdown menu	Yes	3	Specifies number of fail attempts of Health Monitor before interface is torn down.
Attempts Before WAN Recovery	N/A	N/A	N/A	N/A
Priority	Number	Yes	0	Defines that the higher value is higher priority.
Minimum ifup Interval	Dropdown menu	Yes	300 sec	Specifies minimum interval between two successive interface start attempts.
Interface Start Timeout	Dropdown menu	Yes	40 sec	Sets time for interface to startup.
Signal Threshold (dBm)	Dropdown menu	Yes	-115	Specifies the threshold where if the signal is lower than this then it is marked as fail.

When you have configured your settings, click **Save & Apply**.

In the top menu, select **System -> Reboot**. The System page appears.

Figure 58: The reboot page

Check the **Reboot now** check box and then click **Reboot**.

18.3.2 PMP + roaming: pre-empt disabled

As in the previous section, multi-WAN connects the primary predefined interface and uses auto created interfaces. However, in this scenario, the auto created interface will not be disconnected as soon as the primary interface is available. The primary interface will be reconnected when auto created interface is down and when the ifup_retry_sec timeout expires.

The only change in configuration compared to the PMP + roaming: pre-empt enabled example above, is that the pre-empt option in the multi-WAN package must be disabled.

To disable PMP + roaming pre-empt, in the top menu, select **Network -> Multi-Wan**.

In the Multi-WAN page, ensure Preempt is not selected.

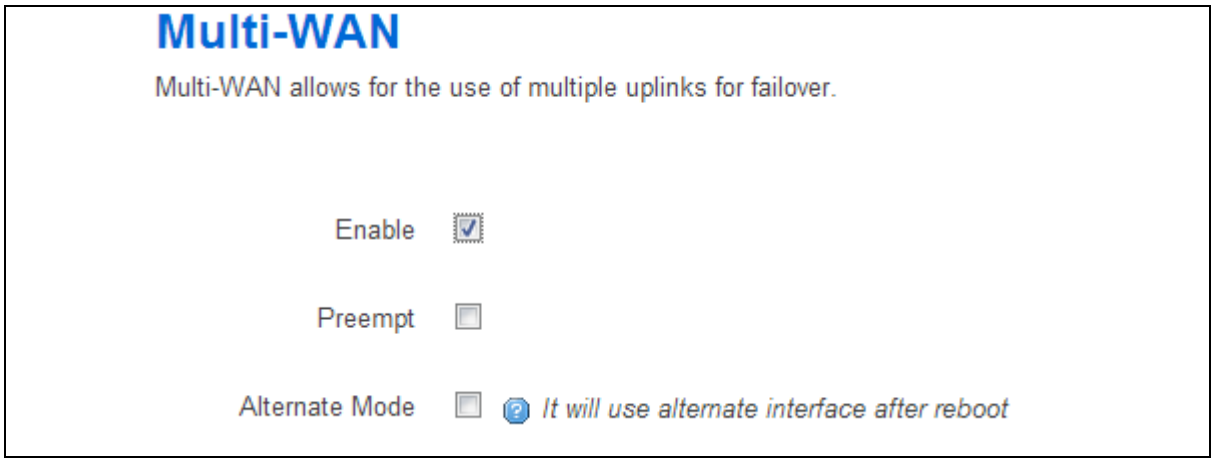


Figure 59: The multi-wan page, pre-empt not selected

Click **Save & Apply**.

In the top menu, select **System -> Reboot**. The System Reboot page appears.

System
Reboot
Reboots the operating system of your device
Reboot now
Reboot on 1970 - January - 1 00 : 00 Reboot
Powered by LuCI Trunk (trunk+svn8382) 15.00.32 image1 config2

Figure 60: The system reboot page

Check the **Reboot now** check box and then click **Reboot**.

18.3.3 Roaming: no PMP defined

There is no primary interface that can be used for a connection. The router uses the network that offers the best signal threshold.

Multi-WAN operation

1. Connect to the first roaming operator interface.
2. Check for signal strength every 'health_interval'. If the signal goes down below 'signal_threshold'
3. Disconnect from first roaming interface
4. Connect to second roaming operator interface.
5. Check for signal strength every 'health_interval'. Stays there until signal goes below 'signal_threshold'
6. Disconnect from second roaming interface. Go to 1.

From the top menu, select **Network -> Multi-Wan**. The Multi-WAN page appears.

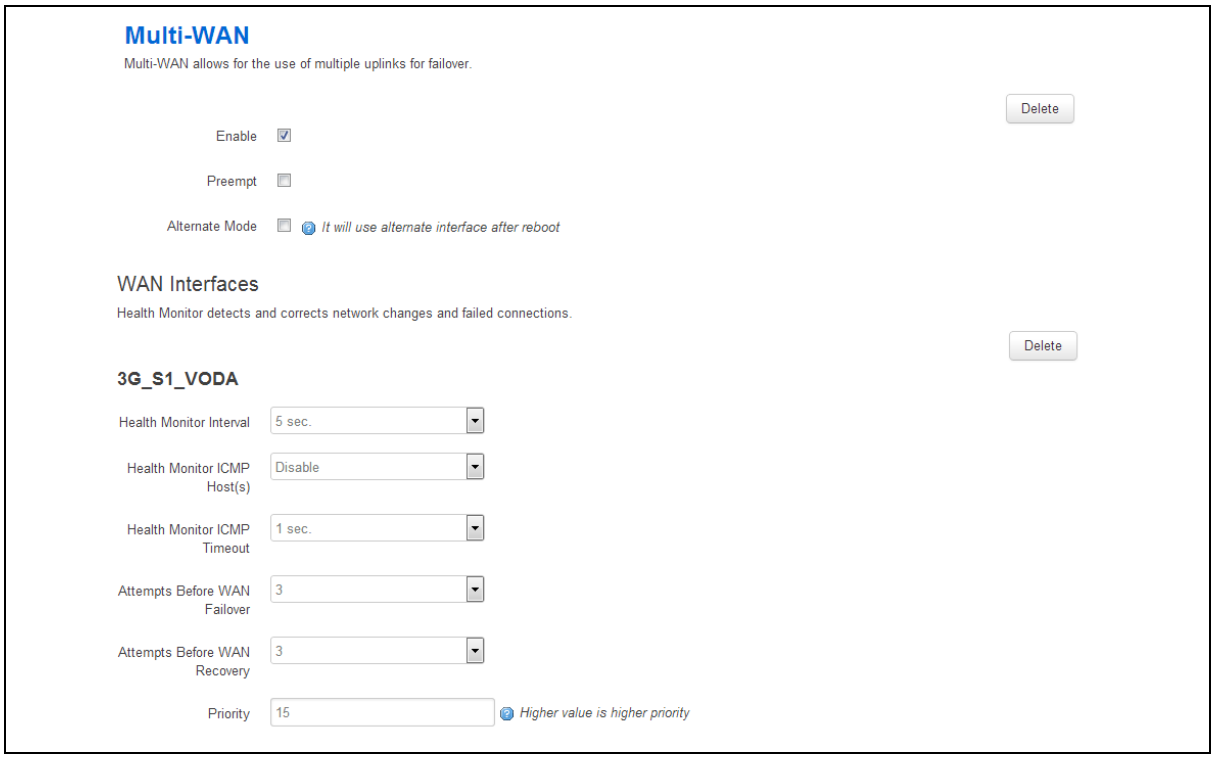


Figure 61: The multi-WAN page

Scroll to the WAN Interfaces section, and click **Delete** to delete predefined Interface.

Click **Save & Apply**.

18.3.4 Disable roaming

There may be occasion where it is desirable to disable roaming. Use UCI on the command line to set the operator option value.

```
cd/etc/config
uci set network.Wan2.operator=’foobar’
uci commit
```

Note: your changes will not take effect without the uci commit command.

To check the settings, enter:

```
cat network
```

```
config interface ‘wan’
        option proto '3g'
        option service 'umts'
        option apn '3ireland.ie’
        option device /dev/ttyACM0’
        option sim '1'
        option pincode '9999'
        option username 'root'
        option password 'admin'
        option operator '3ireland’

config interface ‘Wan2’
        option proto '3g'
        option device /dev/ttyACM1’
        option service 'umts'
        option sim '2'
        option apn ‘foobar’
        option username 'root'
        option password 'admin'
        option operator 'foobar’
root@VA_router:/etc/config1#
```

Apply the ‘operator’ option to both interfaces where both SIMs are used.

© Virtual Access 2015

19 Configuring IPSec

IPSec tunnels are handled by strongSwan.

You must configure three sections:

- Common settings
- Connection settings
- Secret settings

Common settings control the overall behaviour of strongSwan. Together, the connection and secret sections define the required parameters for a two way IKEv1 tunnel.

19.1 Common settings

These settings control the overall behaviour of strongSwan. This behaviour is common across all tunnels.

Name	Type	Required	Default	Description
Enable StongSwan IPSec	Boolean	Yes	No	Enables or disables IPSec.
strictcrlpolicy	boolean	yes	no	Defines if a fresh CRL must be available for the peer authentication based on RSA signatures to succeed.
cachecrls	boolean	yes	no	Shows Certificate Revocation Lists (CRLs) fetched via http or ldap will be cached in /etc/ipsec.d/crls/ under a unique file name derived from the certification authority's public key.
Uniqueids	boolean	yes	yes	Defines whether a particular participant ID should be kept unique, with any new (automatically keyed) connection using an ID from a different IP address deemed to replace all old ones using that ID. Participant IDs normally are unique, so a new (automatically-keyed) connection using the same ID is almost invariably intended to replace an old one.

An example of a typical set of common settings for strongSwan is shown below.

```
root@VA_router:~# uci show Strongswan.general
Strongswan.general=general
Strongswan.general.strictcrlpolicy=no
Strongswan.general.cachecrls=no
Strongswan.general.uniqueids=yes
Strongswan.general.ikev1enabled=yes

config 'general' 'general'
      option 'strictcrlpolicy' 'no'
      option 'cachecrls' 'no'
      option 'uniqueids' 'yes'
```

19.2 Connection settings

Use this section to define the parameters for an IPSec tunnel.

Name	Type	Required	Default	Description
type	string	yes	tunnel	Defines whether the connection is tunnel or transport mode.
name	string	yes	none	Specifies a name for the tunnel.
waniface	string	yes	none	Defines the wan interface used by this tunnel.
xauth_identity	string	No	none	Defines Xauth ID.
authby	String	No	psk	Defines authentication method. Available options, psk, xauthpsk.
Aggressive	String	No	No	Enables aggressive mode
localid	string	Yes	None	Defines the local peer identifier.
locallan	string	Yes	None	Defines the local IP of LAN.
locallanmask	string	Yes	None	Defines the subnet of local LAN.
remoteid	string	Yes	None	Sets the remote peer identifier.
remoteaddress	string	Yes	None	Sets the public IP address of remote peer.
remotelan	string	Yes	None	Sets the IP address of LAN serviced by remote peer.
remotelanmask	string	Yes	None	Sets the Subnet of remote LAN.
Ike	string	Yes	aes128-sha1-modp2048,3des-	Specifies the IKE algorithm to use. The format is: encAlgo-authAlgo-DHGroup encAlgo: 3des, aes, serpent, twofish, blowfish authAlgo: md5, sha, sha2

			sha1-modp1536	DHGroup: modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, modp8192 For example: aes128-sha-modp1536.
esp	string	Yes	aes128-sha1,3des-sha1	Specifies the esp algorithm to use. The format is: encAlgo-authAlgo-PFSGroup encAlgo: 3des, aes, serpent, twofish, blowfish authAlgo: md5, sha, sha2 DHGroup: modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, modp8192 For example: aes128-sha1-modp1536. If no DH group is defined then PFS is disabled.
auto	string	Yes	ignore	Specifies how the tunnel is initiated: start: on startup route: when traffic routes this way. Add: loads a connection without starting it. ignore: ignores the connection.
ikelifetime	string	yes	3h	Specifies how long the keying channel of a connection (ISAKMP or IKE SA) should last before being renegotiated. Syntax: timespec: 1d, 2h, 25m, 10s.
keylife	string	yes	1h	Specifies how long a particular instance of a connection (a set of encryption/authentication keys for user packets) should last, from successful negotiation to expiry. Normally, the connection is renegotiated (via the keying channel) before it expires (see rekeymargin). Syntax: timespec: 1d, 2h, 25m, 10s.
rekeymargin	string			Specifies how long before connection expiry or keying-channel expiry should attempt to

		yes	9m	negotiate a replacement begin. Relevant only locally, other end need not agree on it Syntax: timespec: 1d, 2h, 25m, 10s.
keyingtries	integer	yes	3	Specifies how many attempts (a positive integer or %forever) should be made to negotiate a connection, or a replacement for one, before giving up. The value %forever means 'never give up'. Relevant only locally, other end need not agree on it.
dpdaction	string	string	none	Valid values are none, hold and clear. None: Disables dead peer detection Clear: Clear down the tunnel if peer does not respond. Reconnect when traffic brings the tunnel up. Hold: Clear down the tunnel and bring up as soon as the peer is available. Restart: restarts DPD when no activity is detected
dpddelay	string	yes	30s	Defines the period time interval with which R_U_THERE messages/INFORMATIONAL exchanges are sent to the peer. These are only sent if no other traffic is received. Syntax: timespec: 1d, 2h, 25m, 10s.
dpdtimeout	string	yes	150s	Defines the timeout interval, after which all connections to a peer are deleted in case of inactivity. Syntax: timespec: 1d, 2h, 25m, 10s.

A typical tunnel configuration is shown below.

```
Strongswan.@connection[0]=connection
Strongswan.@connection[0].type=tunnel
Strongswan.@connection[0].name=test
Strongswan.@connection[0].waniface=wan
Strongswan.@connection[0].localid=10.1.1.1
```

```
Strongswan.@connection[0].locallan=10.1.1.0
Strongswan.@connection[0].locallanmask=255.255.255.0
Strongswan.@connection[0].remoteid=10.2.2.2
Strongswan.@connection[0].remoteaddress=10.2.2.2
Strongswan.@connection[0].remotelan=10.2.2.2
Strongswan.@connection[0].remotelanmask=255.255.255.0
Strongswan.@connection[0].ike=3des-md5-modp1024
Strongswan.@connection[0].esp=3des-md5
Strongswan.@connection[0].auto=start
Strongswan.@connection[0].ikelifetime=8h
Strongswan.@connection[0].keylife=1h
Strongswan.@connection[0].rekeymargin=9m
Strongswan.@connection[0].keyingtries=3
Strongswan.@connection[0].dpdaction=hol
Strongswan.@connection[0].dpddelay=30s
Strongswan.@connection[0].dpdtimeout=120s
Strongswan.@connection[0].enabled=yes
config 'connection'
      option enabled 'yes'
      option 'type' 'tunnel'
      option 'name' "test"
      option 'waniface' 'wan'option 'localid' "10.1.1.1"
      option 'locallan' "10.1.1.1"
      option 'locallanmask' "255.255.255.0"
      option 'remoteid' "10.2.2.2"
      option 'remoteaddress' "10.2.2.2"
      option 'remotelan' "10.2.2.2"
      option 'remotelanmask' "255.255.255.0"
      option 'ike' "3des-md5-modp1024"
      option 'esp' "3des-md5"

      option 'auto' 'start'
      option 'ikelifetime' "8h"
      option 'keylife' "1h"
      option 'rekeymargin' "9m"
      option 'keyingtries' "3"
      option 'dpdaction' "hold"
```

```
      option 'dpddelay' "30s"
      option 'dpdtimeout' "120s"
```

19.3 Shunt connection

If the remote LAN network is 0.0.0.0/0 then all traffic generated on the local LAN will be sent via the IPSec tunnel. This includes the traffic destined to the router's IP address. To avoid this situation you must include an additional config connection section.

```
strongswan.@connection[1]=connection
strongswan.@connection[1].name=local
strongswan.@connection[1].enabled=yes
strongswan.@connection[1].locallan=10.1.1.1
strongswan.@connection[1].locallanmask=255.255.255.255
strongswan.@connection[1].remotelan=10.1.1.0
strongswan.@connection[1].remotelanmask=255.255.255.0
strongswan.@connection[1].type=pass
strongswan.@connection[1].auto=route

config connection
        option name 'local'
        option enabled 'yes'
        option locallan '10.1.1.1'
        option locallanmask '255.255.255.255'
        option remotelan '10.1.1.0'
        option remotelanmask '255.255.255.0'
        option type 'pass'
        option auto 'route'
```

Traffic originated on remotelan and destined to locallan address is excluded from VPN IPSec policy.

19.4 Secret settings

Each tunnel also requires settings for how the local end point of the tunnel proves its identity to the remote end point.

Name	Type	Required	Default	Description
enabled	string	Yes	No	Defines whether this set of credentials is to be used or not.
Idtype	String	No	ipaddress	Defines whether IP address or userfqdn is used.
Userfqdn	String	No	None	FQDN or Xauth name. This must match xauth_identity from the config 'connection' section.
localaddress	string	Yes	None	Sets the local ID address.
remoteaddress	string	Yes	None	Sets the remote ID address.
secrettype	string	Yes	psk	Specifies different mechanisms to allow the two peers to authenticate one another. psk: pre-shared secret pubkey: public key signatures rsasig: RSA digital signatures ecdsasig: Elliptic Curve DSA signatures xauth: extended authentication
secret	string			Sets preshared key.

A sample secret section which could be used with the connection section in 'Connection Settings', is shown below:

```
Strongswan.@secret[0]=secret
Strongswan.@secret[0].enabled=yes
Strongswan.@secret[0].localaddress=10.1.1.1
Strongswan.@secret[0].remoteaddress=10.2.2.2
Strongswan.@secret[0].secrettype=psk
Strongswan.@secret[0].secret=secret
config 'secret'
      option 'enabled' "yes"

      option 'localaddress' "10.1.1.1"
      option 'remoteaddress' "10.2.2.2"
      option 'secrettype' 'psk'
      option 'secret' "secret"
```

If xauth is defined as the authentication method then you must include an additional config secret section, as shown in the example below.

```
strongswan.@secret[1].enabled=yes
strongswan.@secret[1].idtype=userfqdn
strongswan.@secret[1].userfqdn=testxauth
strongswan.@secret[1].remoteaddress=10.2.2.2
strongswan.@secret[1].secret=xauth
strongswan.@secret[1].secrettype=XAUTH
config secret
        option enabled 'yes'
        option idtype 'userfqdn'
        option userfqdn 'testxauth'
        option remoteaddress '10.2.2.2'
        option secret 'xauth'
        option secrettype 'XAUTH'
```

20 Configuring firewall

The firewall itself is not required. It is a set of scripts which configure netfilter. If preferred, you can use netfilter directly to achieve the desired firewall behaviour.

Note: the UCI firewall exists to simplify the configuration of netfilter (for many scenarios) without requiring the knowledge to deal with the complexity of netfilter.

The firewall configuration consists of several zones covering one or more interfaces. Allowed traffic flow between the zones is controlled by forwardings. Each zone can include multiple rules and redirects.

Below is an overview of the section types that may be defined in the firewall configuration. A minimal firewall configuration for a router usually consists of one defaults section, at least two zones (LAN and WAN) and one forwarding to allow traffic from LAN to WAN. Other sections that exist are redirects, rules and includes.

20.1 Defaults section

The defaults section declares global firewall settings which do not belong to any specific zones. The following options are defined within this section:

Name	Type	Required	Default	Description
syn_flood	boolean	no	1	Enables SYN flood protection.
drop_invalid	boolean	no	1	Drops packets not matching any active connection.
disable_ipv6	boolean	no	0	Disables IPv6 firewall rules if set to 1.
input	string	no	DROP	Default policy (ACCEPT, REJECT, DROP) for the INPUT chain.
forward	string	no	DROP	Default policy (ACCEPT, REJECT, DROP) for the FORWARD chain.
output	string	no	DROP	Default policy (ACCEPT, REJECT, DROP) for the FORWARD chain.

20.2 Zones section

A zone section groups one or more interfaces and serves as a source or destination for forwardings, rules and redirects. Masquerading (NAT) of outgoing traffic is controlled on a per-zone basis.

The options below are defined within zone sections:

Name	Type	Required	Default	Description
name	zone name	yes	(none)	Sets the unique zone name.
network	list	no	(none)	Defines a list of interfaces attached to this

				zone, if omitted, the value of name is used by default.
masq	boolean	no	0	Specifies whether outgoing zone traffic should be masqueraded (NATTED) - this is typically enabled on the wan zone.
masq_src	list of subnets	no	0.0.0.0/0	Limits masquerading to the given source subnets. Negation is possible by prefixing the subnet with !, multiple subnets are allowed.
masq_dest	list of subnets	no	0.0.0.0/0	Limits masquerading to the given destination subnets. Negation is possible by prefixing the subnet with!, multiple subnets are allowed.
conntrack	boolean	no	1if masquerading is used, 0 otherwise	Forces connection tracking for this zone.
mtu_fix	boolean	no	0	Enables MSS clamping for outgoing zone traffic.
input	string	no	DROP	Default policy (ACCEPT, REJECT, DROP) for incoming zone traffic.
forward	string	no	DROP	Default policy (ACCEPT REJECT, DROP) for forwarded zone traffic.
output	string	no	DROP	Default policy (ACCEPT REJECT, DROP) for outgoing zone traffic.
family	string	no	any	Defines protocol family (ipv4, ipv6 or any) to generate iptables rules for.
log	boolean	no	0	Creates log rules for rejected and dropped traffic in this zone.
log_limit	string	no	10/minute	Limits the amount of log messages per interval.

20.3 Forwarding sections

The forwarding sections control the traffic flow between zones and can enable MSS clamping for specific directions. Only one direction is covered by a forwarding rule. To allow bidirectional traffic flows between two zones, you need two forwardings, with src and dest reversed in each.

The table below shows allowed options within forwarding sections:

Name	Type	Required	Default	Description
src	zone name	yes	(none)	Specifies the traffic source zone, must refer to one of the defined zone names.
dest	zone name	yes	(none)	Specifies the traffic destination zone, must refer to one of the defined zone names.
family	string	no	any	Defines protocol family (ipv4, ipv6 or any) to generate iptables rules for.

The iptables rules generated for this section rely on the state match which needs connection tracking to work. At least one of the src or dest zones needs to have connection tracking enabled through either the masq or the conntrack option.

20.4 Redirects

Port forwardings (DNAT) are defined by redirect sections. All incoming traffic on the specified source zone which matches the given rules will be directed to the specified internal host.

The options described in the table below are valid for redirects:

Name	Type	Required	Default	Description
src	zone name	yes for DNAT target	(none)	Specifies the traffic source zone, must refer to one of the defined zone names. For typical port forwards, this is usually wan.
rc_ip	ip address	no	(none)	Matches incoming traffic from the specified source IP address.
src_dip	ip address	yes for SNAT target	(none)	For DNAT, matches incoming traffic directed at the given destination ip address. For SNAT rewrites the source address to the given address.
src_mac	mac address	no	(none)	Matches incoming traffic from the specified mac address.
src_port	port or range	no	(none)	Matches incoming traffic originating from the given source port or port range on the client host.
src_dport	port or range	no	(none)	For DNAT, matches incoming traffic directed at the given destination port or port range on this host. For SNAT rewrites the source ports to the given value.
proto	protocol name or number	yes	tcpudp	Matches incoming traffic using the given protocol.
dest	zone name	yes for SNAT target	(none)	Specifies the traffic destination zone, must refer to one of the defined zone names.
dest_ip	ip address	yes for DNAT target	(none)	For DNAT, redirects matched incoming traffic to the specified internal host. For SNAT, matches traffic directed at the given address.
dest_port	port or range	no	(none)	For DNAT, redirects matched incoming traffic to the given port on the internal host. For SNAT, matches traffic directed at the given ports.
target	string	no	DNAT	NAT target (DNAT or SNAT) to use when generating the rule.
family	string	no	any	Protocol family (ipv4, ipv6 or any) to generate iptables rules for.
reflection	boolean	no	1	Disables NAT reflection for this redirect if set to 0 - applicable to DNAT targets.

© Virtual Access 2015

limit	string	no	(none)	Sets maximum average matching rate; specified as a number, with an optional /second, /minute, /hour or /day suffix. Example 3/hour.
limit_burst	integer	no	5	Sets maximum initial number of packets to match. This number gets recharged by one every time the limit specified above is not reached, up to this number.
extra	string	no	(none)	Extra arguments to pass to iptables, this is useful to specify additional match options, like-m policy --dir in for IPSec.

20.5 Rules

Sections of the type rule can be used to define basic accept or reject rules to allow or restrict access to specific ports or hosts. Like redirects the rules are tied to the given source zone and match incoming traffic occurring there.

Valid options for this section are:

Name	Type	Required	Default	Description
src	zone name	yes	(none)	Specifies the traffic source zone, must refer to one of the defined zone names.
src_ip	ip address	no	(none)	Match incoming traffic from the specified source IP address.
src_mac	mac address	no	(none)	Match incoming traffic from the specified mac address.
src_port	port or range	no	(none)	Match incoming traffic originating from the given source port or port range on the client host if tcp or udp is specified as protocol.
proto	protocol name or number	no	tcpudp	Match incoming traffic using the given protocol. Can be one of tcp, udp, tcpudp, udplite, icmp, esp, ah, sctp, or all or it can be a numeric value, representing one of these protocols or a different one. A protocol name from /etc/protocols is also allowed. The number 0 is equivalent to all.
Dest	zone name	no	(none)	Specifies the traffic destination zone, must refer to one of the defined zone names. If specified, the rule applies to forwarded traffic else it is treated as input rule.
dest_ip	ip address	no	(none)	Match incoming traffic directed to the specified destination IP address.
dest_port	port or range	no	(none)	Match incoming traffic directed at the given destination port or port range on this host if tcp or udp is specified as protocol.
target	string	yes	DROP	Firewall action (ACCEPT, REJECT, DROP) for matched traffic.
family	string	no	any	Protocol family (ipv4, ipv6 or any) to generate iptables rules for.

limit	string	no	(none)	Maximum average matching rate; specified as a number, with an optional /second, /minute, /hour or /day suffix. Example3/hour.
limit_burst	integer	no	5	Maximum initial number of packets to match; this number gets recharged by one every time the limit specified above is not reached, up to this number.
extra	string	no	(none)	Extra arguments to pass to iptables, this is mainly useful to specify additional match options, like -m policy --dir in for IPSec.

20.6 Includes

It is possible to include custom firewall scripts by specifying one or more include sections in the firewall configuration.

There is only one possible parameter for includes:

Name	Type	Required	Default	Description
path	file name	yes	/etc/firewall.user	Specifies a shell script to execute on boot or firewall restarts.

Included scripts may contain arbitrary commands, for example advanced iptables rules or tc commands required for traffic shaping.

When writing custom iptables rules use –I (insert) instead of –A (append) to ensure that the created rules appear before the generic ones.

20.7 IPv6 notes

As described above, the option family is used for distinguishing between IPv4, IPv6 and both protocols. However, the family is inferred automatically if IPv6 addresses are used, for example is automatically treated as IPv6 only rule:

```
config rule
        option src wan
        option src_ip fdca:f00:ba3::/64
        option target ACCEPT
```

Similarly, such a rule is automatically treated as IPv4 only.

```
config rule
        option src wan
        option dest_ip 88.77.66.55
        option target REJECT
```

Rules without IP addresses are automatically added to iptables and ip6tables, unless overridden by the family option. Redirect rules (port forwards) are always IPv4 since there is no IPv6 DNAT support at present.

20.8 Implications of DROP vs. REJECT

The decision whether to drop or to reject traffic should be done on a case-by-case basis. Many people see dropping traffic as a security advantage over rejecting it because it exposes less information to a hypothetical attacker. While dropping slightly increases security, it can also complicate the debugging of network issues or cause unwanted side-effects on client programs.

If traffic is rejected, the router will respond with an icmp error message ("destination port unreachable") causing the connection attempt to fail immediately. This also means that for each connection attempt a certain amount of response traffic is generated. This can actually harm if the firewall is attacked with many simultaneous connection attempts, the resulting backfire of icmp responses can clog up all available upload and make the connection unusable (DoS).

When connection attempts are dropped the client is not aware of the blocking and will continue to re-transmit its packets until the connection eventually times out. Depending on the way the client software is implemented, this could result in frozen or hanging programs that need to wait until a timeout occurs before they're able to continue.

DROP

- less information is exposed
- less attack surface
- client software may not cope well with it (hangs until connection times out)
- may complicate network debugging (where was traffic dropped and why)

REJECT

- may expose information (like the IP at which traffic was actually blocked)
- client software can recover faster from rejected connection attempts
- network debugging easier (routing and firewall issues clearly distinguishable)

20.9 Note on connection tracking

By default, the firewall will disable connection tracking for a zone if no masquerading is enabled. This is achieved by generating NOTRACK firewall rules matching all traffic passing via interfaces referenced by the firewall zone. The purpose of NOTRACK is to speed up routing and save memory by circumventing resource intensive connection tracking in cases where it is not needed. You can check if connection tracking is disabled by issuing iptables -t raw -vnL, it will list all rules, check for NOTRACK target.

NOTRACK will render certain iptables extensions unusable, for example the MASQUERADE target or the state match will not work.

If connection tracking is required, for example by custom rules in /etc/firewall.user, the conntrack option must be enabled in the corresponding zone to disable NOTRACK. It should appear as option 'conntrack' '1' in the right zone in /etc/config/firewall.

20.10 Firewall examples

20.10.1 Opening ports

The default configuration accepts all LAN traffic, but blocks all incoming WAN traffic on ports not currently used for connections or NAT. To open a port for a service, add a rule section:

```
config rule
        option src              wan
        option dest_port        22
        option target           ACCEPT
        option proto            tcp
```

This example enables machines on the Internet to use SSH to access your router.

20.10.2 Forwarding ports (destination NAT/DNAT)

This example forwards http, but not HTTPS, traffic to the web server running on 192.168.1.10:

```
config redirect
        option src       wan
        option src_dport 80
        option proto     tcp
        option dest_ip   192.168.1.10
```

The next example forwards one arbitrary port that you define to a box running ssh behind the firewall in a more secure manner because it is not using default port 22.

```
config 'redirect'
        option 'name' 'ssh'
        option 'src' 'wan'
        option 'proto' 'tcpudp'
        option 'src_dport' '5555'
        option 'dest_ip' '192.168.1.100'
        option 'dest_port' '22'
        option 'target' 'DNAT'
        option 'dest' 'lan'
```

20.10.3 Source NAT (SNAT)

Source NAT changes an outgoing packet destined for the system so that is looks as though the system is the source of the packet.

Define source NAT for UDP and TCP traffic directed to port 123 originating from the host with the IP address 10.55.34.85. The source address is rewritten to 63.240.161.99.

```
config redirect
        option src              lan
        option dest             wan
        option src_ip           10.55.34.85
        option src_dip          63.240.161.99
        option dest_port        123
        option target           SNAT
```

When used alone, Source NAT is used to restrict a computer's access to the Internet, but allows it to access a few services by manually forwarding what appear to be a few local services; for example, NTP to the Internet. While DNAT

hides the local network from the Internet, SNAT hides the Internet from the local network.

Source NAT and destination NAT are combined and used dynamically in IP masquerading to make computers with private (192.168.x.x, etc.) IP addresses appear on the Internet with the system's public WAN IP address.

20.10.4 True destination port forwarding

This usage is similar to SNAT, but as the destination IP address is not changed, machines on the destination network need to be aware that they'll receive and answer requests from a public IP address that is not necessarily theirs. Port forwarding in this fashion is typically used for load balancing.

```
config redirect
        option src              wan
        option src_dport        80
        option dest             lan
        option dest_port        80
        option proto            tcp
```

20.10.5 Block access to a specific host

The following rule blocks all connection attempts to the specified host address.

```
config rule
        option src              lan
        option dest             wan
        option dest_ip          123.45.67.89
        option target           REJECT
```

20.10.6 Block access to the internet using MAC

The following rule blocks all connection attempts from the client to the internet.

```
config rule
        option src              lan
        option dest             wan
        option src_mac          00:00:00:00:00:00
        option target           REJECT
```

20.10.7 Block access to the internet for specific IP on certain times

The following rule blocks all connection attempts to the internet from 192.168.1.27 on weekdays between 21:00pm and 09:00am.

```
config rule
        option src              lan
        option dest             wan
        option src_ip           192.168.1.27
        option extra            '-m time --weekdays Mon,Tue,Wed,Thu,Fri --
timestart 21:00 --timestop 09:00'
        option target           REJECT
```

20.10.8 Restricted forwarding rule

The example below creates a forward rule rejecting traffic from LAN to WAN on the ports 1000-1100.

```
config rule
        option src              lan
        option dest             wan
        option dest_port        1000-1100
        option proto            tcpudp
        option target           REJECT
```

20.10.9 Transparent proxy rule (same host)

The rule below redirects all outgoing HTTP traffic from LAN through a proxy server listening at port 3128 on the router itself.

```
config redirect
      option src              lan
      option proto            tcp
      option src_dport        80
      option dest_port        3128
```

20.10.10 Transparent proxy rule (external)

The following rule redirects all outgoing HTTP traffic from LAN through an external proxy at 192.168.1.100 listening on port 3128. It assumes the router LAN address to be 192.168.1.1 - this is needed to masquerade redirected traffic towards the proxy.

```
config redirect
        option src              lan
        option proto            tcp
        option src_ip           !192.168.1.100
        option src_dport        80
        option dest_ip          192.168.1.100
        option dest_port        3128
        option target           DNAT

config redirect
        option dest             lan
        option proto            tcp
        option src_dip          192.168.1.1
        option dest_ip          192.168.1.100
        option dest_port        3128
        option target           SNAT
```

20.10.11 Simple DMZ rule

The following rule redirects all WAN ports for all protocols to the internal host 192.168.1.2.

```
config redirect
      option src              wan
      option proto            all
      option dest_ip          192.168.1.2
```

20.10.12 IPSec passthrough

This example enables proper forwarding of IPSec traffic through the WAN.

```
# AH protocol
config rule
        option src              wan
        option dest             lan
        option proto            ah
        option target           ACCEPT
```

```
# ESP protocol
config rule
        option src              wan
        option dest             lan
        option proto            esp
        option target           ACCEPT
```

For some configurations you also have to open port 500/UDP.

```
# ISAKMP protocol
config rule
        option src              wan
        option dest             lan
        option proto            udp
        option src_port         500
        option dest_port        500
        option target           ACCEPT
```

20.10.13 Manual iptables rules

You can specify traditional iptables rules, in the standard iptables unix command form, in an external file and included in the firewall config file. It is possible to use this process to include multiple files.

```
config include
       option path /etc/firewall.user


config include
       option path /etc/firewall.vpn
```

The syntax for the includes is Linux standard and therefore different from UCIs. The syntax documentation can be found in netfilter.

20.11 Firewall management

After a configuration change, firewall rules are rebuilt by entering:

```
root@VA_router:/# /etc/init.d/firewall restart
```

Executing the following command will flush all rules and set the policies to ACCEPT on all standard chains:

```
root@VA_router:/# /etc/init.d/firewall stop
```

To manually start the firewall, enter:

```
root@VA_router:/# /etc/init.d/firewall start
```

The firewall can be permanently disabled by enter:

```
root@VA_router:/# /etc/init.d/firewall disable
```

Note: disable does not flush the rules, so you might be required to issue a stop before.

To enable the firewall again enter:

```
root@VA_router:/# /etc/init.d/firewall enable
```

20.12 Debug generated rule set

It is possible to observe the iptables commands generated by the firewall programme. This is useful to track down iptables errors during firewall restarts or to verify the outcome of certain UCI rules.

To see the rules as they are executed, run the fw command with the FW_TRACE environment variable set to 1 (one):

```
root@VA_router:/# FW_TRACE=1 fw reload
```

To direct the output to a file for later inspection, enter:

```
root@VA_router:/# FW_TRACE=1 fw reload 2>/tmp/iptables.lo
```

21 Configuring SNMP

The SNMP daemon has several configuration sections that configure the agent itself (agent and system sections), assignment of community names and which SNMP protocols are in use to groups (com2sec and group sections), creation of views and subviews (access section) of the whole available SNMP tree and finally, granting specific access to those views on a group by group basis (access section).

21.1 agent

The options defined for this section are outlined below.

Name	Type	Required	Description
agentaddress	string	yes	Specifies the address(es) and port(s) on which the agent should listen. [(udp|tcp):]port[@address][,...]
authtrapenabled	boolean yes|no	no	yes: enables SNMP authentication trap no: disables SNMP authentication trap Note this is the SNMP poll authentication trap, to be sent when there is a community mismatch
link_updown_notify	boolean yes|no	no	when enabled the router sends a trap notifying link up/down

A typical sample agent configuration is shown below. It causes the agent to listen on udp port 161, with authentication traps and notify link up/down enabled.

```
uci set snmpd.@agent[0].agentaddress=UDP:161
uci set snmpd.@agent[0].authtrapenabled=1
uci set snmpd.@agent[0].link_updown_notify=yes

config 'agent'
      option agentaddress 'UDP:161'
      option authtrapenabled '1'
      option link_updown_notify 'yes'
```

Another sample agent configuration shown below causes the agent to listen on udp port 161, tcp port 161 and udp port 9161 on only the interface associated with the localhost address.

```
config 'agent'
      option agentaddress 'UDP:161,tcp:161,9161@localhost'
```

21.2 system

The options defined for this section are shown in the table below.

Name	Type	Required	Description
agentaddress	string	yes	Specifies the address(es) and port(s) on which the agent should listen. [(udp|tcp):]port[@address][,...]
sysLocation	string	yes	Sets the system location, system contact or system name for the agent. This information is reported in the 'system' group the mibII tree.
sysContact	string	yes	Ordinarily these objects (sysLocation.0, sysContact.0 and sysName.0) are read-write.
sysName	string	yes	However, specifying the value for one of these objects by giving the appropriate token makes the corresponding object read-only, and attempts to set the value of the object will result in a notWritable error response.

A possible system configuration section is shown below:

```
config 'system'
      option sysLocation 'Office 123'
      option sysContact 'Mr White'
      option sysName 'Backup Access 4'
```

21.3 com2sec

This section is used to map SNMP community names into an arbitrary security name. Mapping of community names into security names is done based on the community name and the source subnet. The first source/community combination that matches the incoming packet is used.

The options defined for this section are outlined below.

Name	Type	Required	Description
secname	string	yes	Specifies an arbitrary security name for the user.
source	string	yes	A hostname, localhost or a subnet specified as a.b.c.d/mask or a.b.c.d/bits.
community	string	yes	The community string being presented in the request.

The following sample specifies that a request from any source using “public” as the community string will be dealt with using the security name “ro”. However,

any request from the localhost itself using “private” as the community string will be dealt with using the security name “rw”.

Note: the security names of “ro” and “rw” here are simply names – the fact of a security name having read only or read-write permissions is handled in the access section and dealt with at a group granularity.

```
config 'com2sec' 'public'
      option secname 'ro'
      option source 'default'
      option community 'public'

config 'com2sec' 'private'
      option secname 'rw'
      option source 'localhost'
      option community 'private'
group
```

The options defined for this section are outlined below.

Name	Type	Required	Description
group	string	yes	Specifies an arbitrary group name.
version	string	yes	Specifies the SNMP version number being used in the request: v1, v2c and usm are supported.
secname	string	yes	An already defined security name that is being included in this group.

The following example specifies that a request from the security name “ro” using snmp v1, v2c or USM (User Based Security Model for SNM P v3) are all mapped to the “public” group. Similarly, requests from the security name “rw” in all protocols are mapped to the “private” group.

```
config 'group' 'public_v1'
      option group 'public'
      option version 'v1'
      option secname 'ro'

config 'group' 'public_v2c'
      option group 'public'
      option version 'v2c'
      option secname 'ro'
```

```
config 'group' 'public_usm'
      option group 'public'
      option version 'usm'
      option secname 'ro'

config 'group' 'private_v1'
      option group 'private'
      option version 'v1'
      option secname 'rw'

config 'group' 'private_v2c'
      option group 'private'
      option version 'v2c'
      option secname 'rw'

config 'group' 'private_usm'
      option group 'private'
      option version 'usm'
      option secname 'rw'
```

The options defined for this section are outlined below.

Name	Type	Required	Description
viewname	string	yes	Specifies an arbitrary view name. Typically it describes what the view shows.
type	string	yes	Specifies whether the view lists oids that are included in the view or lists oids to be excluded from the view (in which case all other oids are visible apart from those ones listed). Values: included, excluded
oid	string	yes	An oid: 1: is everything .iso.org.dod.Internet.mgmt.mib-2: mib2 Any other valid oid

The following example defines two views, one for the entire system and another for only mib2.

```
config 'view' 'all'
      option viewname 'all'
      option type 'included'
      option oid '.1'

config 'view' 'mib2'
      option viewname 'mib2'
      option type 'included'
      option oid '.iso.org.dod.Internet.mgmt.mib-2'
```

21.4 access

The options defined for this section are outlined below.

Name	Type	Required	Description
group	string	yes	Specifies the group to which access is being granted.
context	string	yes	For SNMP v1 and SNMP v2c context must be none.
version	string	yes	Specifies the SNMP version number being used in the request: any, v1, v2c and usm are supported.
level	string	yes	The security level: noauth, auth or priv. For SNMP v1 and SNMP v2c level must be noauth.
Prefix	string	yes	Prefix specifies how context (above) should be matched against the context of the incoming pdu, either exact or prefix.
Read	A valid view or none	yes	Specifies the view to be used for read access.
Write	A valid view or none	yes	Specifies the view to be used for write access.
Notify	A valid view or none	yes	Specifies the view to be used for notify access.

The following example shows the “public” group being granted read access on the “all” view and the “private” group being granted read and write access on the “all” view.

```
config 'access' 'public_access'
      option group 'public'
      option context 'none'
      option version 'any'
      option level 'noauth'
```

```
      option prefix 'exact'
      option read 'all'
      option write 'none'
      option notify 'none'

config 'access' 'private_access'
      option group 'private'
      option context 'none'
      option version 'any'
      option level 'noauth'
      option prefix 'exact'
      option read 'all'
      option write 'all'
      option notify 'all'
```

21.5 SNMP traps

The options defined for this section are outlined below.

```
# for SNMPv1 or v2c trap receivers
config trapreceiver
   option host 'IPADDR[:PORT]'
   option version 'v1|v2c'
   option community 'COMMUNITY STRING'
# for SNMPv2c inform request receiver

config informreceiver
   option host 'IPADDR[:PORT]'
   option community 'COMMUNITY STRING'
An additional option was added to the 'agent' subsection:
   option authtrapenabled '0|1
```

22 Configuring HTTP server

The uhttpd configuration is used by the uhttpd web server package. This file defines the behaviour of the server and default values for certificates generated for SSL operation. uhttpd supports multiple instances, that is, multiple listen ports, each with its own document root and other features, as well as cgi, and lua.

There are two sections defined, the section of type uhttpd contains general server settings while the cert section defines the default values for SSL certificates.

22.1 Server settings

The options defined for this section are outlined below.

Name	Type	Required	Default	Description
listen_http	list of port numbers or address:port pairs	yes	(none)	Specifies the ports and addresses to listen on for plain HTTP access. If only a port number is given, the server will attempt to serve both IPv4 and IPv6 requests. Use 0.0.0.0.:80 to bind at port 80 only on IPv4 interfaces or [::] : 80 to serve only IPv6.
listen_https	list of port numbers or address:port pairs	no	(none)	Specifies the ports and addresses to listen on for encrypted HTTPS access. The format is the same as for listen_http. Read below for extra details.
Home	directory path	yes	/www	Defines the server document root.
Cert	file path	yes if listen_ https is given, else no	/etc/ uhttpd.crt	ASN.1/DER certificate used to serve HTTPS connections
key	file path	yes if listen_ https is given, else no	/etc/ uhttpd.key	ASN.1/DER private key used to serve HTTPS connections.
cgi_prefix	string	no	/cgi-bin	Defines the prefix for CGI scripts, relative to the document root. CGI support is disabled if this option is missing.
lua_prefix	string	no	(none)	Defines the prefix for dispatching requests to the embedded Lua interpreter, relative to the

				document root. Lua support is disabled if this option is missing.
lua_handler	file path	yes if lua_ prefix is given, else no	(none)	Specifies Lua handler script used to initialize the Lua runtime on server start.
script_timeout	integer	no	60	Sets maximum wait time for CGI or Lua requests in seconds. Requested executables are terminated if no output was generated until the timeout expired.
network_timeout	integer	no	30	Sets maximum wait time for network activity. Requested executables are terminated and connection is shut down if no network activity occurred for the specified number of seconds.
realm	string	no	local hostname	Defines basic authentication realm when prompting the client for credentials (HTTP 400).
config	file path	no	/etc/ httpd.conf	Config file in Busybox httpd format for additional settings (currently only used to specify Basic Auth areas).
index_page	file name	no	index.html, index.htm, default.html, default.htm	Index file to use for directories, e.g. add index.php when using php.
error_page	string	no	(none)	Virtual URL of file or CGI script to handle 404 request. Must begin with '/'
no_symlinks	boolean	no	0	Do not follow symbolic links if enabled.
no_dirlists	boolean	no	0	Do not generate directory listings if enabled.

Multiple sections of the type uhttpd may exist - the init script will launch one webserver instance per section.

A standard uhttpd configuration is shown below.

```
root@VA_router:~# uci show uhttpd.main
uhttpd.main=uhttpd

uhttpd.main.listen_http=0.0.0.0:80
uhttpd.main.listen_https=0.0.0.0:443
uhttpd.main.home=/www
uhttpd.main.rfc1918_filter=1
uhttpd.main.cert=/etc/uhttpd.crt
uhttpd.main.key=/etc/uhttpd.key
uhttpd.main.cgi_prefix=/cgi-bin
uhttpd.main.script_timeout=60
uhttpd.main.network_timeout=30

config 'uhttpd' 'main'
      list 'listen_http' '0.0.0.0:80'
      list 'listen_https' '0.0.0.0:443'
      option 'home' '/www'
      option 'rfc1918_filter' '1'
      option 'cert' '/etc/uhttpd.crt'
      option 'key' '/etc/uhttpd.key'
      option 'cgi_prefix' '/cgi-bin'
      option 'script_timeout' '60'
      option 'network_timeout' '30'
```

22.2 HTTPS certificate settings and creation

If listen_https is defined in the server configuration and the certificate and private key is missing, the web server init script will generate the appropriate certificate and key files when the server is started for the first time, either by reboot or by manual restart.

The uhttpd configuration contains a section detailing the certificate and key files creation parameters.

Name	Type	Required	Default	Description
days	integer	no	730	Validity time of the generated certificates in days.
bits	integer	no	1024	Size of the generated RSA key in bits.
country	string	no	DE	ISO country code of the certificate issuer.
state	string	No	Berlin	State of the certificate issuer.

Location	string	no	Berlin	Location/city of the certificate issuer.
commonname	string	no	(none)	Common name covered by the certificate. For the purposes of secure Activation this MUST be set to the serial number (eth0 mac address) of the device.

A standard uhttp certificate section is shown below.

```
root@VA_router:~# uci show uhttpd.px5g
uhttpd.px5g=cert
uhttpd.px5g.days=3650
uhttpd.px5g.bits=1024
uhttpd.px5g.country=IE
uhttpd.px5g.state=Dublin
uhttpd.px5g.location=Dublin
uhttpd.px5g.commonname=00E0C8000000

config 'cert' 'px5g'
      option 'days' '3650'
      option 'bits' '1024'
      option 'country' 'IE'
      option 'state' 'Dublin'
      option 'location' 'Dublin'
      option 'commonname' '00E0C8000000'
```

22.3 Basic authentication (httpd.conf)

For backward compatibility reasons, uhttpd uses the file /etc/httpd.conf to define authentication areas and the associated usernames and passwords. This configuration file is not in UCI format.

Authentication realms are defined in the format prefix:username:password with one entry and a line break.

Prefix is the URL part covered by the realm, for example, cgi-bin to request basic auth for any CGI program.

Username specifies the username a client has to login with.

Password defines the secret password required to authenticate.

The password can be either in plain text format, MD5 encoded or in the form $p$user where the user refers to an account in /etc/shadow or /etc/passwd.

If the p… format is used, uhttpd will compare the client provided password against the one stored in the shadow or passwd database.

22.4 Securing uHTTPd

By default, uHTTPd binds to 0.0.0.0 which also includes the WAN port of your router. To bind uHTTPd to the LAN port only you have to change the listen_http and listen_https options to your LAN IP address.

To get your current LAN IP address, enter:

```
uci get network.lan.ipaddr
```

then, modify the configuration appropriately:

```
uci set uhttpd.main.listen_http='192.168.1.1:80'
uci set uhttpd.main.listen_https='192.168.1.1:443'

config 'uhttpd' 'main'
        # HTTP listen addresses, multiple allowed
        list listen_http        192.168.1.1:80
#       list listen_http        [::]:80

        # HTTPS listen addresses, multiple allowed
        list listen_https       192.168.1.1:443
#       list listen_https       [::]:443
```

22.5 SSH server configuration

A sample SSH Server configuration is shown below.

```
root@VA_router:~# uci show dropbear
dropbear.@dropbear[0]=dropbear
dropbear.@dropbear[0].PasswordAuth=on
dropbear.@dropbear[0].RootPasswordAuth=on
dropbear.@dropbear[0].Port=22
root@VA_router:~# uci export dropbear
package 'dropbear'
config 'dropbear'

      option 'PasswordAuth' 'on'
      option 'RootPasswordAuth' 'on'
      option 'Port' '22'
```

23 Configuring ADSL

23.1 What is ADSL technology?

Asymmetric Digital Subscriber Line (ADSL) is a technology for transmitting digital information at high speed on existing telephone lines to homes and businesses. Unlike a regular, dial-up telephone service, ADSL provides a continuously available, ‘always-on’ connection. ADSL was specifically designed to exploit the asynchronous nature of most multimedia communication in which the user can obtain large amounts of information and only a small amount of interactive control information is returned. ADSL circuits can support data rates of up to 8 Mbps downstream from the network service to the user; and 1 Mbps upstream from the user to the network service.

23.2 ADSL connections

ADSL access services typically use the Asynchronous Transfer Mode (ATM) protocol to provide a low level communications path between the user's access equipment and the service provider head end. The head end may be a Broadband Access Server (BAS) that sits, logically, behind the ADSL central office Digital Subscriber Line Access Multiplexer (DSLAM) and is connected using an ATM backbone. ATM is a high-speed switching technology where data is grouped into cells.

Connection between the user equipment and the BAS is then achieved using the Point-to-Point Protocol (PPP) running over the ATM connection path. PPP is a defined industry standard used widely to allow two devices to communicate across a logical link. It is extensively deployed by service providers as a means of connecting customers to Internet Protocol (IP)-based services, such as the Internet.

The method of running PPP between the user equipment and the BAS may be either directly over the ATM layer (PPPoA) or over an intermediate Ethernet layer (PPPoE).

23.3 ADSL connection options on your router

You can configure two main types of ADSL service on your router:

- ADSL routed PPP connection
- ADSL bridged connection

If you select the Routed PPP service, you can run the PPP over ATM (PPPoA) or over Ethernet (PPPOE). The following diagrams illustrate the topology of these connections.

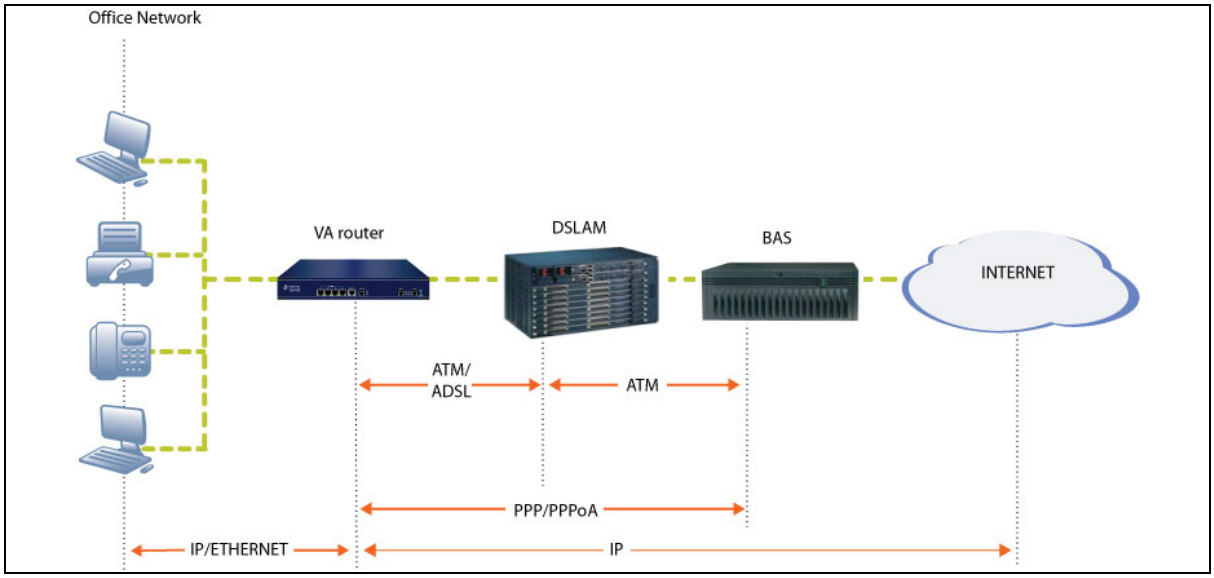


Figure 62: A routed ADSL connection over PPPoA

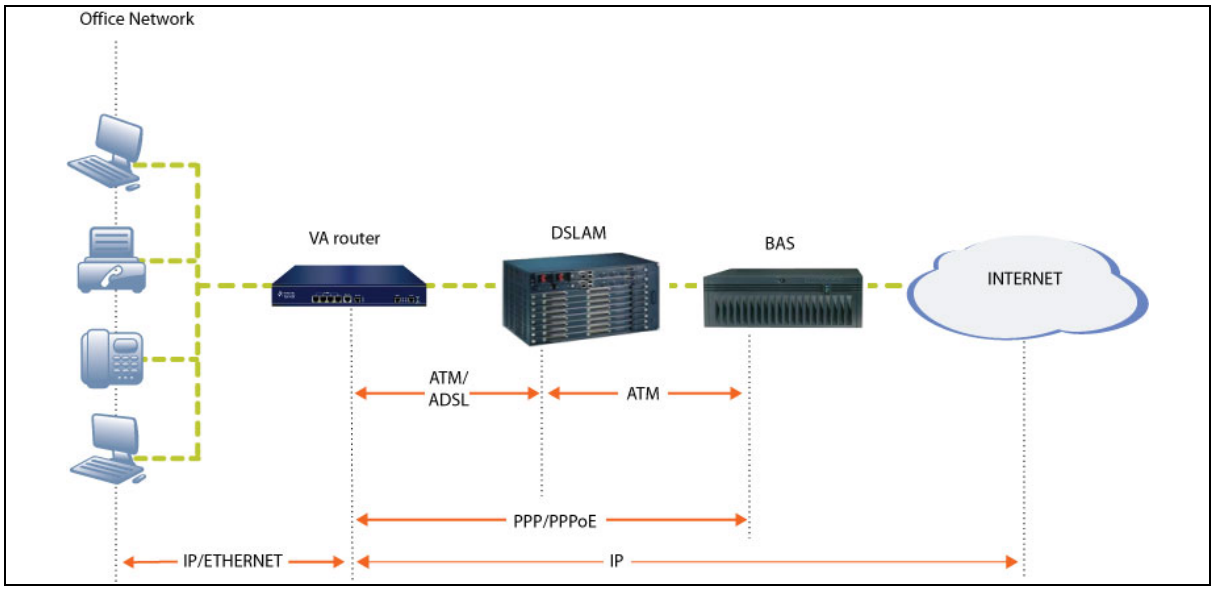


Figure 63: A routed ADSL connection over PPPoE

Less commonly, you may need to configure a bridged connection over ADSL. In this type of configuration the router will be receiving Ethernet packets over the ADSL line and can be configured with an IP address for management.

23.4 Configuring ADSL PPP connection via the web interface

In your Internet browser, type in the local IP address of a router, for example, the default IP address **192.168.100.1** and press enter. The Authorization page appears.

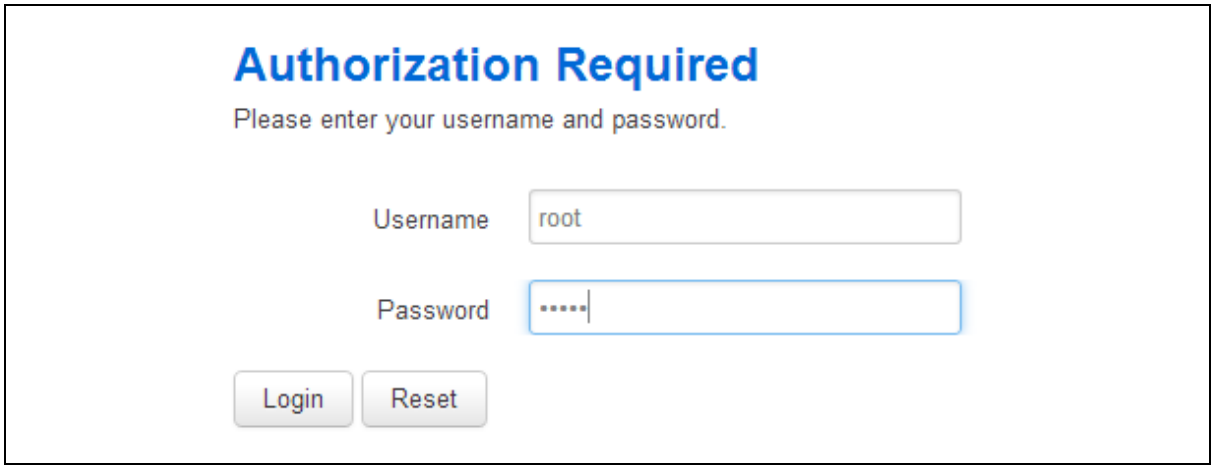


Figure 64: The login page

In the username field, type **root**.

In the Password field, type **admin**.

Click **Login**.

23.5 Configuring an ADSL PPPoA connection

From the top menu select Network -> Interfaces. The Interface Overview page appears.

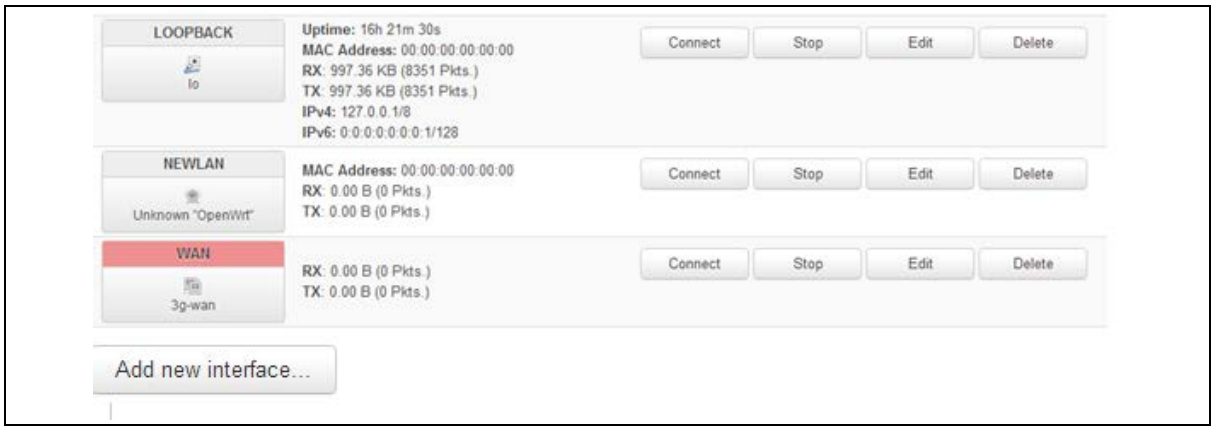


Figure 65: The interfaces overview page

Click **Add new interface....**The Create Interface page appears.

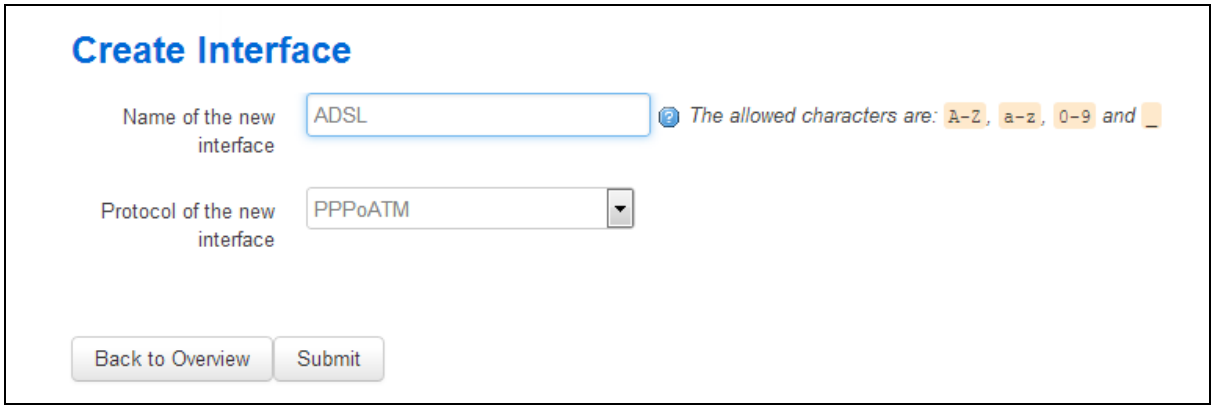


Figure 66: Create Interface page

In the Name of the new interface field, type the name of the **PPPoA interface**.

In the Protocol of the new interface, from the drop-down menu select **PPPoATM**.

Click **Submit**. The ADSL Interfaces page appears.

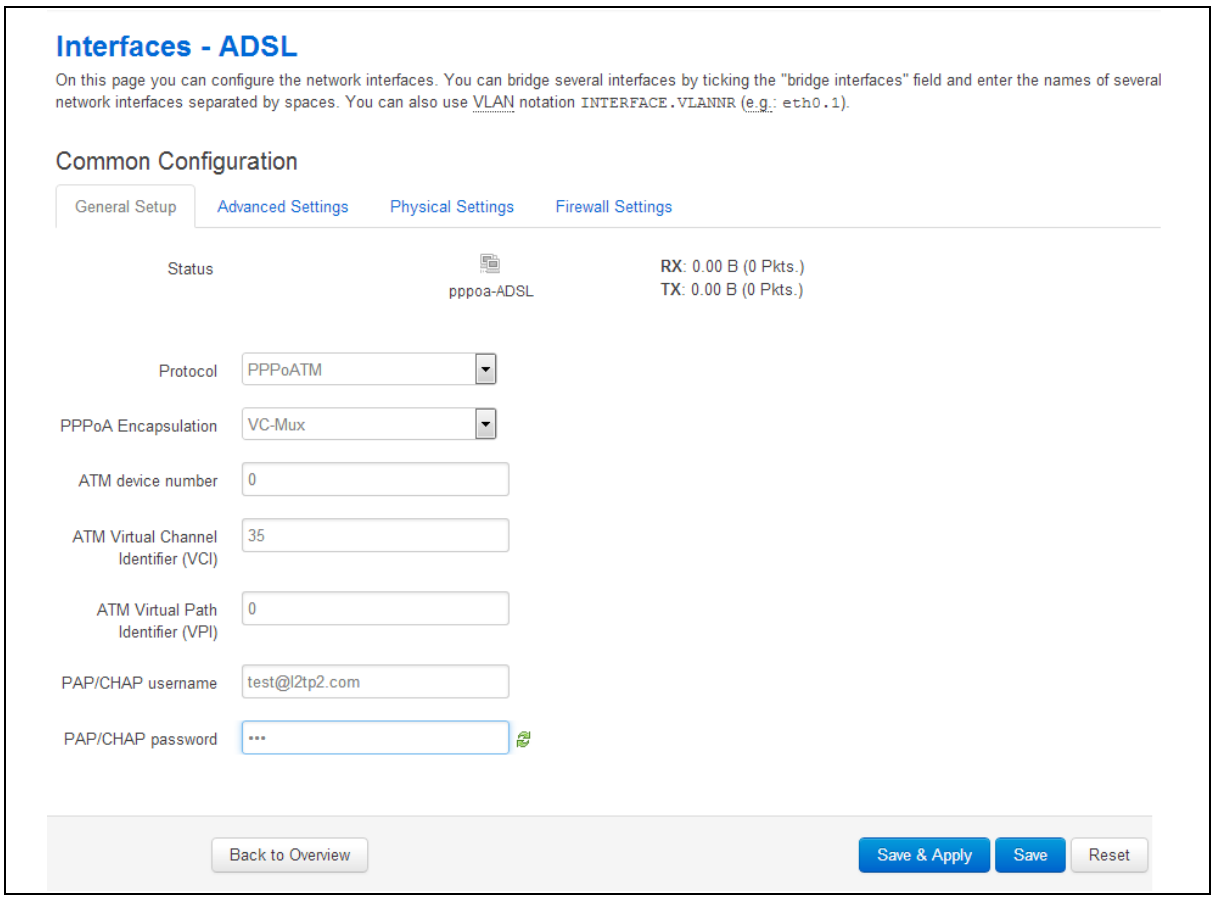


Figure 67: The interface page

From the PPPoA Encapsulation drop-down menu, select **VC-Mux or LLC**.

In the ATM device number field, leave the default value as **0**.

In the Virtual Channel Identifier field, type the **VCI number**.

In the ATM Virtual Path Identifier field, type the **VPI number**.

Select the **Firewall Settings** tab. The ADSL Interfaces page appears.

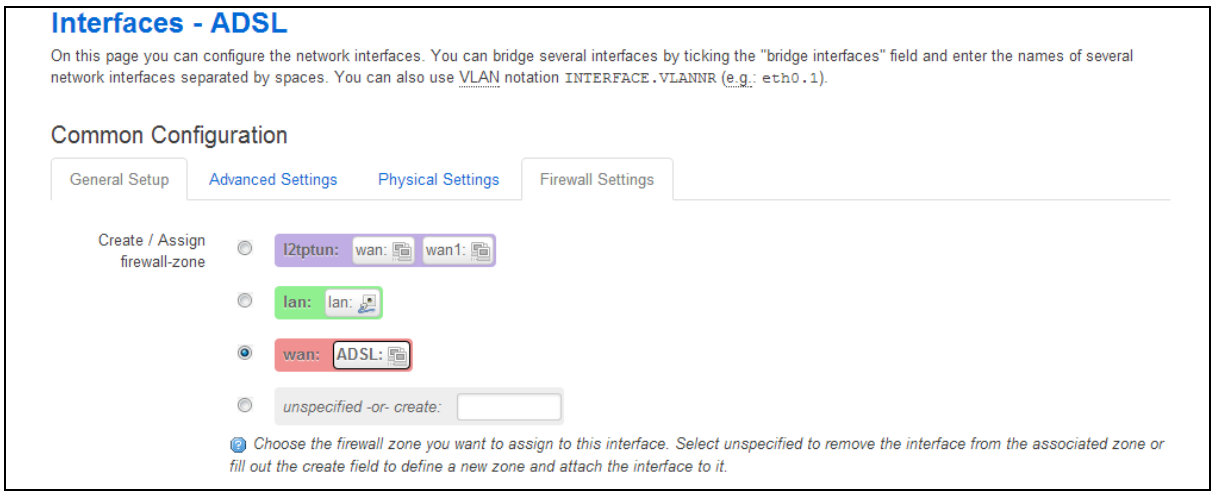

Interfaces - ADSL
On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).
Common Configuration
General Setup
Advanced Settings
Physical Settings
Firewall Settings
Create / Assign firewall-zone
l2tptun: wan: wan1:
lan: lan:
wan: ADSL:
unspecified -or- create:
Choose the firewall zone you want to assign to this interface. Select unspecified to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

Figure 68: The interfaces page firewall section

Check the **Create / Assign firewall-zone** radio button to add the ADSL interface into wan firewall-zone.

Click **Save & Apply**.

23.6 Configuring an ADSL PPPoEoA connection

From the top menu select **Network -> Interfaces**. The Interfaces Overview page appears.

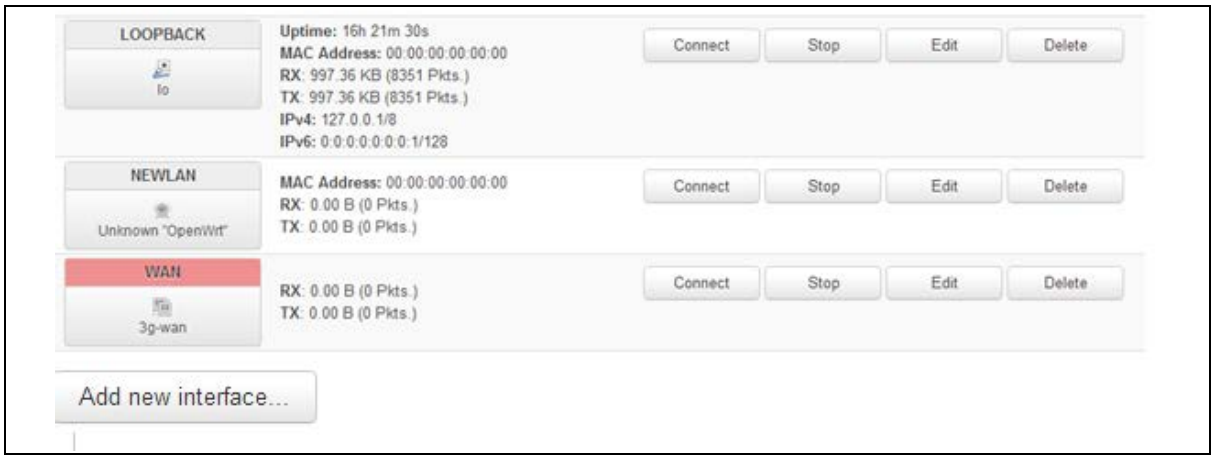


Figure 69: The interfaces overview page

Scroll down to the bottom of the page until you see the ATM Bridges section.

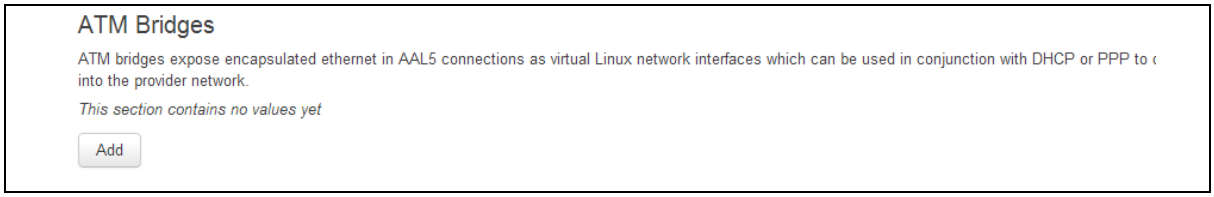

ATM Bridges
ATM bridges expose encapsulated ethernet in AAL5 connections as virtual Linux network interfaces which can be used in conjunction with DHCP or PPP to
into the provider network.
This section contains no values yet
Add

Figure 70: The ATM bridges page

Click **Add**. The ATM Bridges page appears.

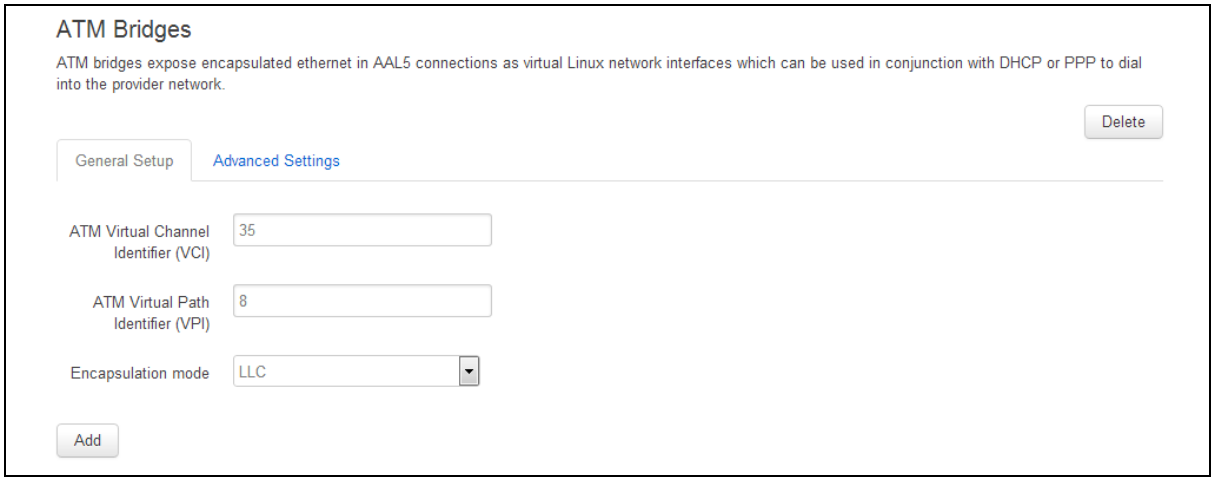

ATM Bridges
ATM bridges expose encapsulated ethernet in AAL5 connections as virtual Linux network interfaces which can be used in conjunction with DHCP or PPP to dial into the provider network.
Delete
General Setup
Advanced Settings
ATM Virtual Channel Identifier (VCI)
35
ATM Virtual Path Identifier (VPI)
8
Encapsulation mode
LLC
Add

Figure 71: The ATM bridges general tab

Select the **General Setup** tab.

In the Virtual Channel Identifier field, type the **VCI number**.

In the ATM Virtual Path Identifier field, type the **VPI number**.

In Encapsulation mode drop-down menu select either **LLC** or **VC-Mux**.

Select the **Advanced Settings** tab. The ATM Bridges page appears.

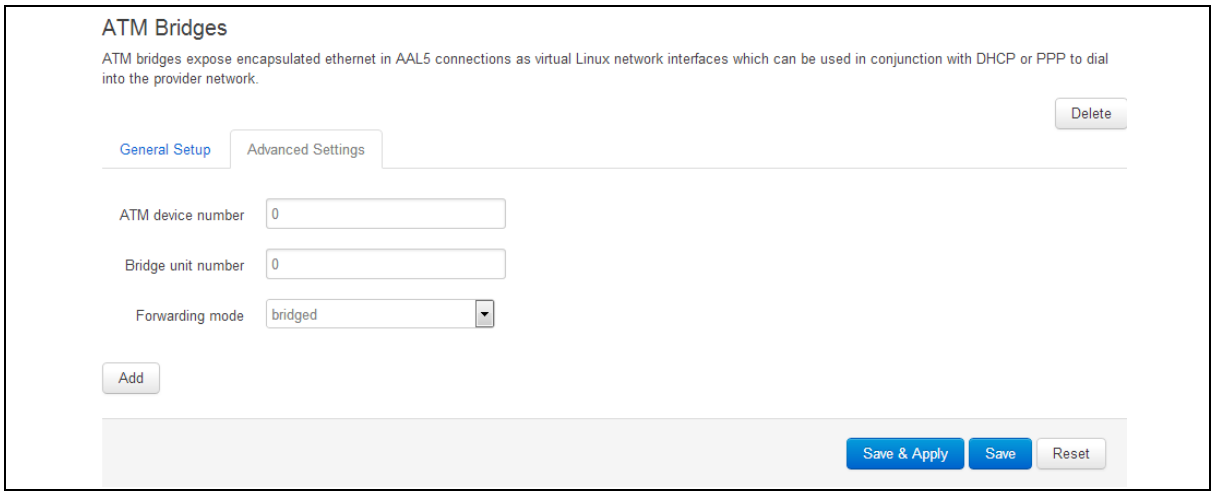


Figure 72: The ATM bridges advanced settings tab

Leave the default ATM device number and the Bridge unit number set to **0**.

In the Forwarding mode drop down menu, select **bridged** or **routed**.

Click **Save**.

Click **Add new interface….**the Create Interface page appears.

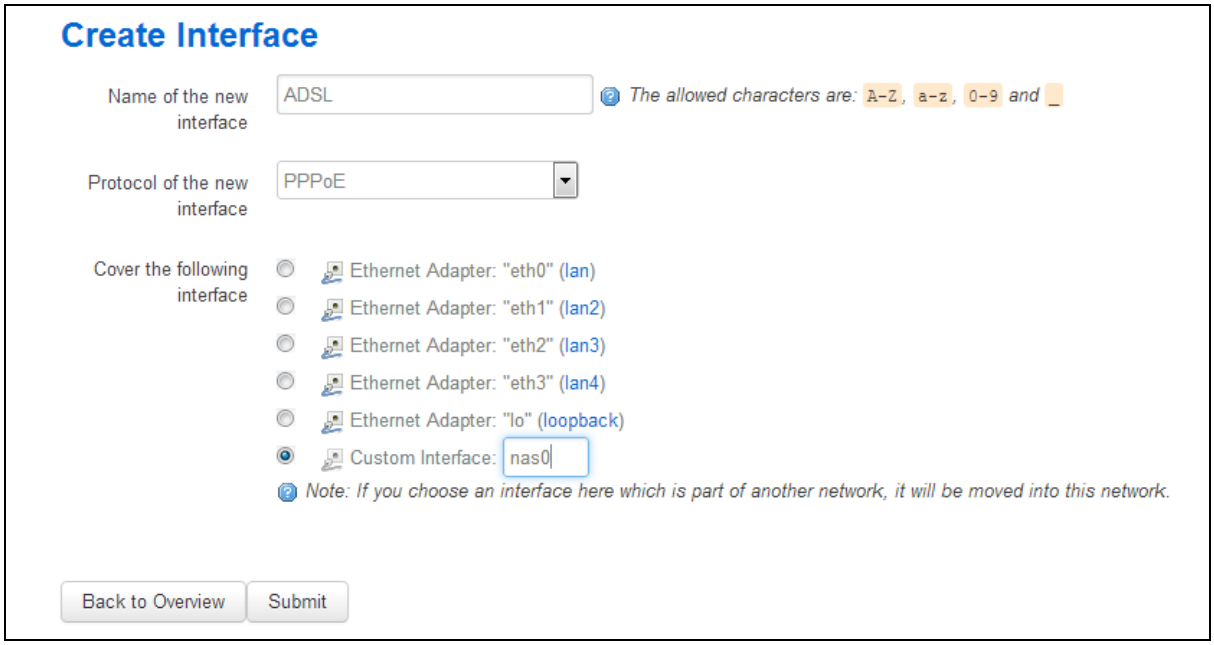

Create Interface
Name of the new interface
ADSL
The allowed characters are: A-Z, a-z, 0-9 and _
Protocol of the new interface
PPPoE
Cover the following interface
Ethernet Adapter: "eth0" (lan)
Ethernet Adapter: "eth1" (lan2)
Ethernet Adapter: "eth2" (lan3)
Ethernet Adapter: "eth3" (lan4)
Ethernet Adapter: "lo" (loopback)
Custom Interface: nas0
Note: If you choose an interface here which is part of another network, it will be moved into this network.
Back to Overview
Submit

Figure 73: The create interface page

In the Name of the new interface field, type the **name of the interface**.

From Protocol of the new interface drop-down menu, select **PPPoE**.

From cover the following interface, select **Custom Interface**, and then type **nas0**.

Click **Submit**. The Interfaces – [name of new interface] page appears.

Figure 74: The new interface page

In the PAP/CHAP username field, type the **CHAP username**.

In the PAP/CHAP password field, type the **password**.

Optionally in Access Concentrator field, type the **AC name**.

Optionally in Service Name field, type the **SA name**.

Select the **Firewall Settings** tab. The Interfaces - [name of new interface] page appears.

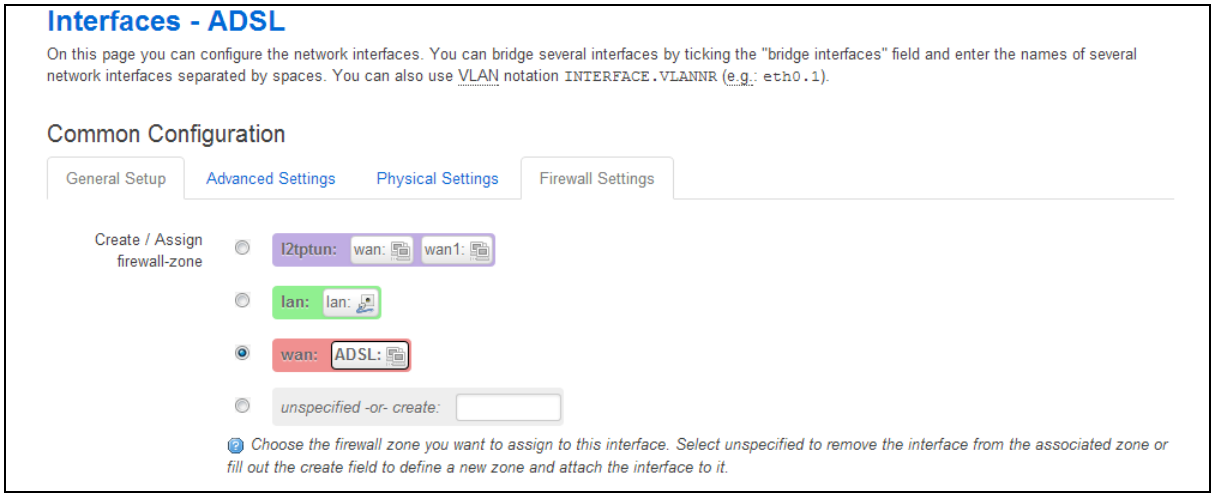

Interfaces - ADSL
On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).
Common Configuration
General Setup
Advanced Settings
Physical Settings
Firewall Settings
Create / Assign firewall-zone
l2tptun: wan: wan1:
lan: lan:
wan: ADSL:
unspecified -or- create:
Choose the firewall zone you want to assign to this interface. Select unspecified to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

Figure 75: The interfaces page firewall settings tab

To add the ADSL interface into wan firewall-zone, select **Create / Assign**.

Click **Save & Apply**.

23.7 Configuring an ADSL bridge connection with static IP

From the top menu select Network -> Interfaces. The Interfaces Overview page appears.

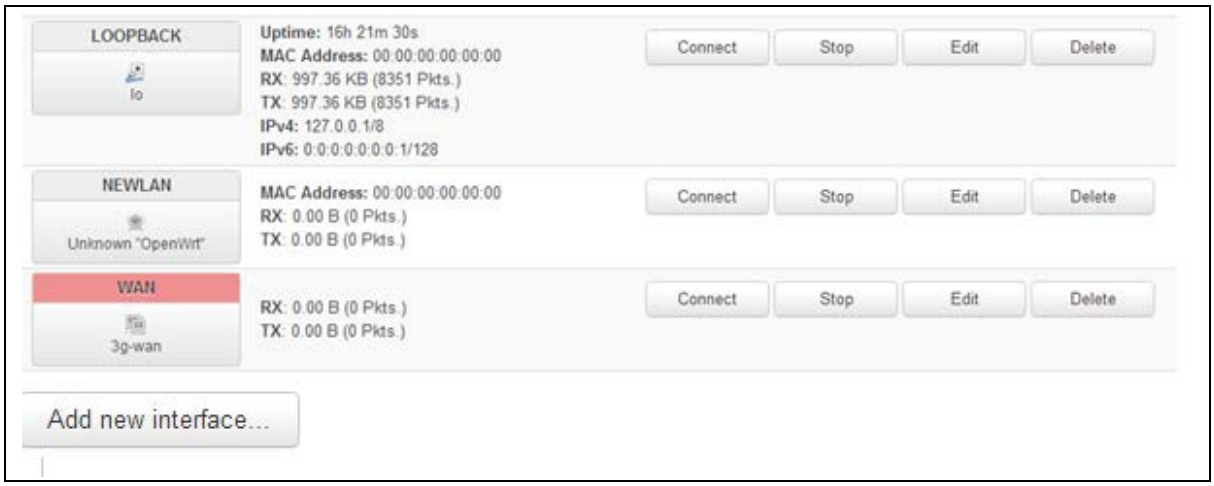


Figure 76: The interfaces overview page

Scroll down to the bottom of the page until you see the ATM Bridges section.

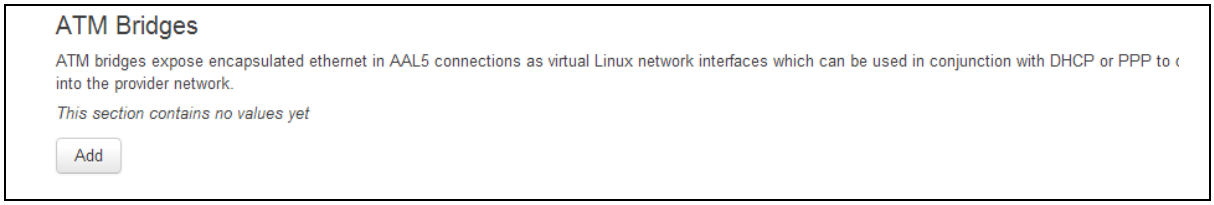

ATM Bridges
ATM bridges expose encapsulated ethernet in AAL5 connections as virtual Linux network interfaces which can be used in conjunction with DHCP or PPP to
into the provider network.
This section contains no values yet
Add

Figure 77: The ATM bridges page

Click Add. The ATM Bridges page appears.

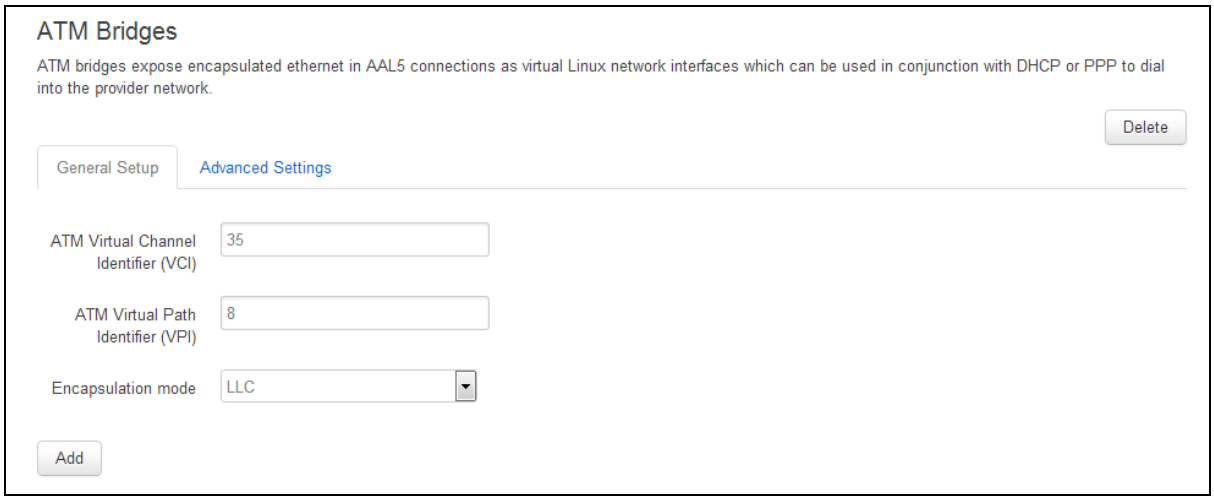

ATM Bridges
ATM bridges expose encapsulated ethernet in AAL5 connections as virtual Linux network interfaces which can be used in conjunction with DHCP or PPP to dial into the provider network.
Delete
General Setup
Advanced Settings
ATM Virtual Channel Identifier (VCI)
35
ATM Virtual Path Identifier (VPI)
8
Encapsulation mode
LLC
Add

Figure 78: The ATM bridges general tab

Select the **General Setup** tab.

In the Virtual Channel Identifier field, type the **VCI number**.

In the ATM Virtual Path Identifier field, type the **VPI number**.

In Encapsulation mode drop-down menu select either **LLC** or **VC-Mux**.

Select the **Advanced Settings** tab. The ATM Bridges page appears.

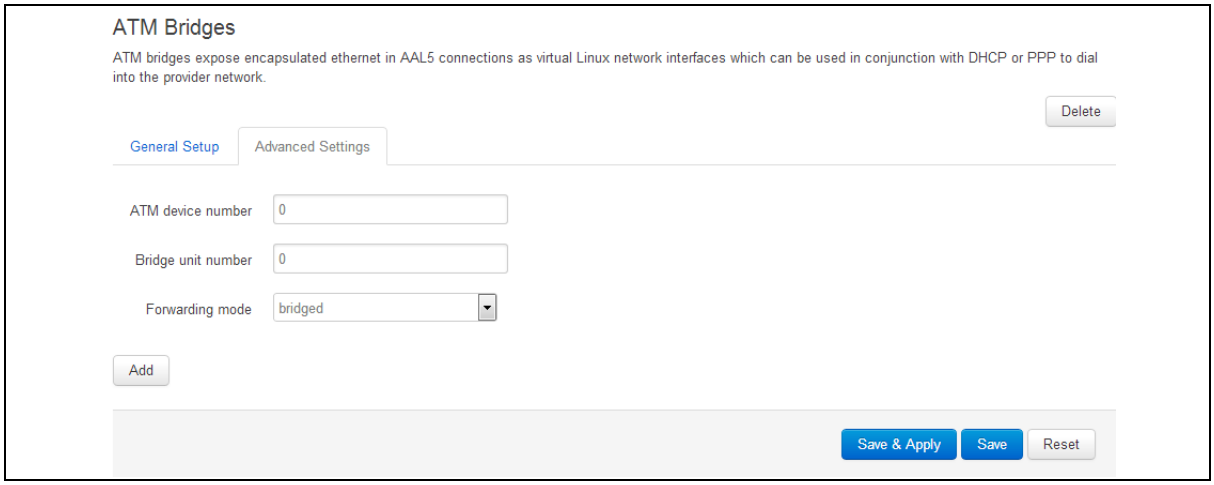


Figure 79: The ATM bridges advanced settings tab

Leave the default ATM device number and the Bridge unit number set to **0**.

In the Forwarding mode drop down menu, select **bridged**.

Click **Save**.

Click **Add new interface….**the Create Interface page appears.

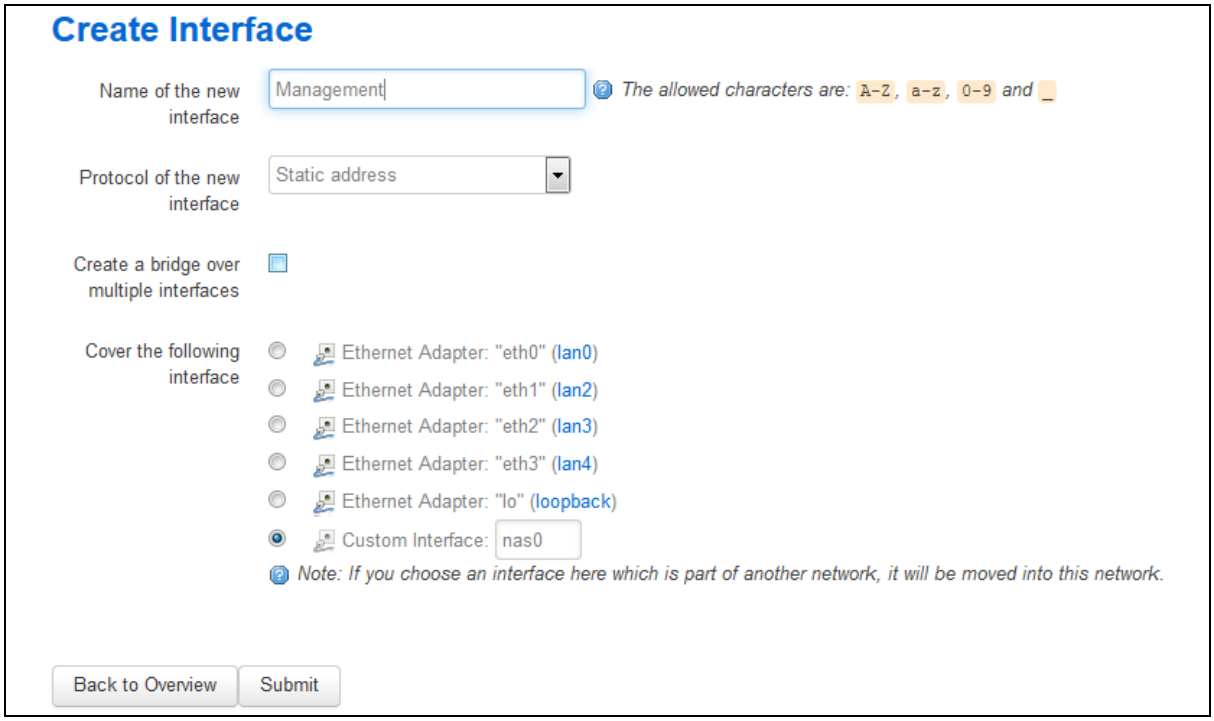

Create Interface
Name of the new interface
Management
The allowed characters are: A-Z, a-z, 0-9 and _
Protocol of the new interface
Static address
Create a bridge over multiple interfaces
Cover the following interface
Ethernet Adapter: "eth0" (lan0)
Ethernet Adapter: "eth1" (lan2)
Ethernet Adapter: "eth2" (lan3)
Ethernet Adapter: "eth3" (lan4)
Ethernet Adapter: "lo" (loopback)
Custom Interface: nas0
Note: If you choose an interface here which is part of another network, it will be moved into this network.
Back to Overview
Submit

Figure 80: The create interface page

In the Name of the new interface field, type the name of the **interface**.

From Protocol of the new interface drop-down menu, select **Static address**.

From cover the following interface, select Custom Interface, and then type **nas0**.

Click **Submit**. The Interfaces – [name of new interface] page appears.

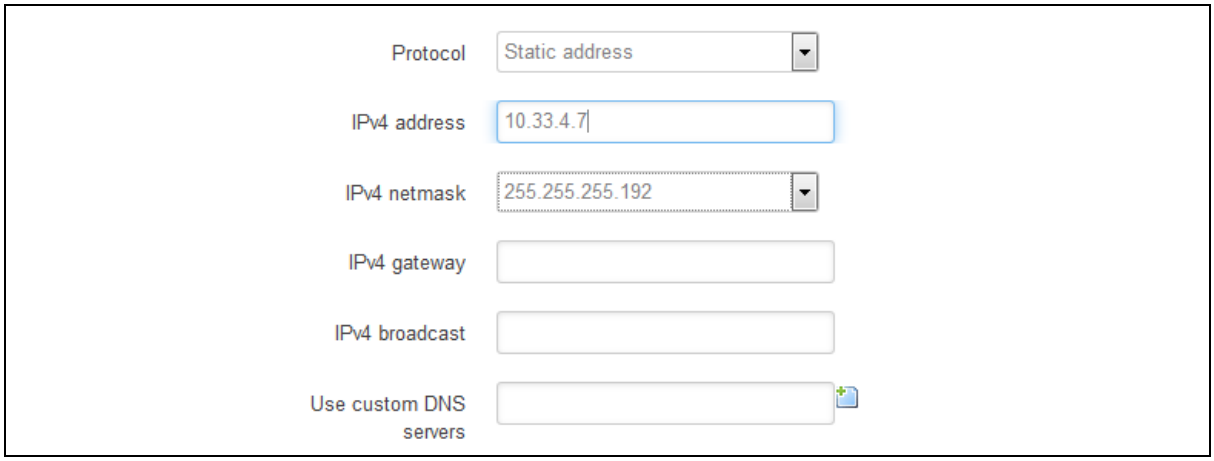


Figure 81: Part of new interface configuration page

In the IPv4 address field, type the **IP address**.

In the IPv4 netmask field, type or choose **netmask**.

Optionally in IPv4 gateway field, type the **gateway address**.

If necessary, fill in other require fields.

Select the **Firewall Settings** tab. The Interfaces - [name of new interface] page appears.

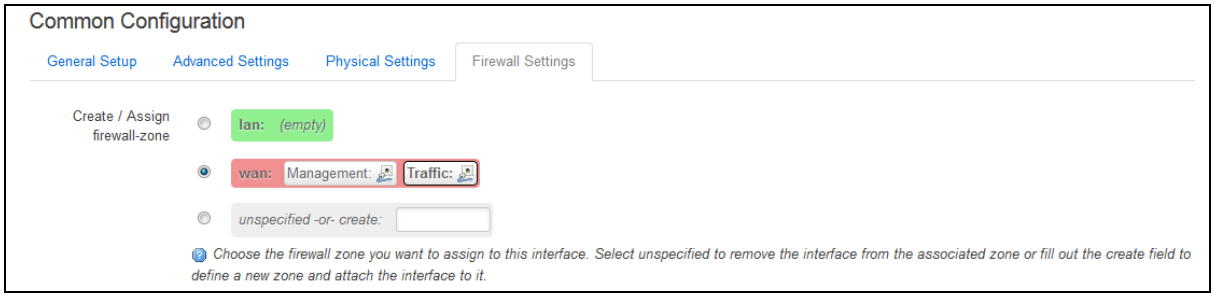

Common Configuration
General Setup
Advanced Settings
Physical Settings
Firewall Settings
Create / Assign firewall-zone
lan: (empty)
wan: Management: Traffic:
unspecified -or- create:
Choose the firewall zone you want to assign to this interface. Select unspecified to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

Figure 82: The interfaces page firewall settings tab

To add the ADSL interface into wan firewall-zone, select **Create / Assign**.

Click **Save & Apply**.

23.8 Configuring ADSL via UCI

23.8.1 Configuring an ADSL PPPoA connection via UCI

The configuration file is stored at:

Network file /etc/config/network

To view the configuration file, type the command:

uci export network

```
config adsl-device 'adsl'
        option fwannex 'a'
        option annex 'a'
        option Enabled 'yes'
config interface 'ADSL'
        option proto 'pppoa'
        option encaps 'vc'
        option atmdev '0'
        option vci '35'
        option vpi '0'
        option username 'test5@pppoa.com'
        option password 'test5'
```

to view uci commands, type:

uci show network

```
network.adsl.fwannex=a
network.adsl.annex=a
network.adsl.Enabled=yes
network.ADSL=interface
network.ADSL.proto=pppoa
network.ADSL.encaps=vc
network.ADSL.atmdev=0
network.ADSL.vci=35
network.ADSL.vpi=0
network.ADSL.username=test5@pppoa.com
network.ADSL.password=test5
```

23.8.2 Configuring an ADSL PPPoEoA connection via UCI

The configuration file is stored at:

Network file /etc/config/network

To view the configuration file, enter:

```
uci export network
config adsl-device 'adsl'
        option fwannex 'a'
        option annex 'a'
        option Enabled 'yes'

config interface 'ADSL'
        option proto 'pppoe'
        option ifname 'nas0'
        option username 'test5@pppoe.com'
        option password 'test5'
        option ac 'test'
        option service 'test'
        option defaultroute '0'
config atm-bridge
        option unit '0'
        option atmdev '0'
```

```
        option encaps 'llc'
        option payload 'bridged'
        option vci '35'
        option vpi '0'

To view uci commands, enter:
uci show network
network.adsl=adsl-device
network.adsl.fwannex=a
network.adsl.annex=a
network.adsl.Enabled=yes
network.ADSL=interface
network.ADSL.proto=pppoe
network.ADSL.ifname=nas0
network.ADSL.username=test5@pppoe.com
network.ADSL.password=test5
network.ADSL.ac=test
network.ADSL.service=test
network.ADSL.defaultroute=0
network.@atm-bridge[0]=atm-bridge
network.@atm-bridge[0].unit=0
network.@atm-bridge[0].atmdev=0
network.@atm-bridge[0].encaps=llc
network.@atm-bridge[0].payload=bridged
network.@atm-bridge[0].vci=35
network.@atm-bridge[0].vpi=0

Configuring an ADSL bridge connection via UCI
The configuration file is stored at:
Network file /etc/config/network
To view the configuration file, type the command:
uci export network
config adsl-device 'adsl'
        option fwannex 'a'
        option annex 'a'
        option enabled 'yes'
```

```
config atm-bridge
        option unit '0'
        option atmdev '0'
        option payload 'bridged'
        option vpi '8'
        option vci '39'
        option encaps 'llc'

config interface 'Management'
        option proto 'static'
        option ifname 'nas0'
        option monitored '0'
        option ipaddr '10.33.4.7'
        option netmask '255.255.255.192'

to view uci commands, type:
uci show network
network.adsl.fwannex=a
network.adsl.annex=a
network.adsl.enabled=yes
network.@atm-bridge[0]=atm-bridge
network.@atm-bridge[0].unit=0
network.@atm-bridge[0].atmdev=0
network.@atm-bridge[0].payload=bridged
network.@atm-bridge[0].vpi=8
network.@atm-bridge[0].vci=39
network.@atm-bridge[0].encaps=llc
network.Management=interface
network.Management.proto=static
network.Management.ifname=nas0
network.Management.monitored=0
network.Management.ipaddr= 10.33.4.7
network.Management.netmask=255.255.255.192
```

© Virtual Access 2015

24 Virtual Router Redundancy Protocol (VRRP)

The Virtual Router Redundancy Protocol (VRRP) is a networking protocol designed to eliminate the single point of failure inherent in the static default routed environment.

VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP router on a LAN. The VRRP router controlling the IP address(es) associated with a virtual router is called the Master, and forwards packets sent to these IP addresses. The election process provides dynamic failover in the forwarding responsibility from the Master to a Backup router should the Master become unavailable.

This process allows the virtual router IP address(es) on the LAN to be used as the default first hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

Two or more routers forming the redundancy cluster are configures with the same Router ID and Virtual IP address. A VRRP router group operates within the scope of the single LAN.

Additionally, the VRRP routers are configured with its initial role (Master or Backup) and the router priority, which is a factor in the master router election process.

A password authentication may also be configured to protect VRRP protocol messages against spoofing.

The VRRP protocol is implemented according to Internet standard RFC2338.

24.1 Software versions

VRRP is available on VIE, ARN, LIS and GIG software versions.

To check which software your router is running, SSH to a router and the following information is shown.

```
Serial Number:  00E0C8121299
Hardware Model: GW7314
Provider:       Virtual Access
Boot Image:     image2 - LIS-15.00.52rc15
Boot Config:    config2
Current Time:   15:26:44 30 Oct 2014 GMT
Uptime:         up 0 min,  load average: 1.69, 0.42, 0.14
```

Figure 83: Example output after accessing the router via SSH

When you are logged in via an SSH session, run the command, vacmd show vars

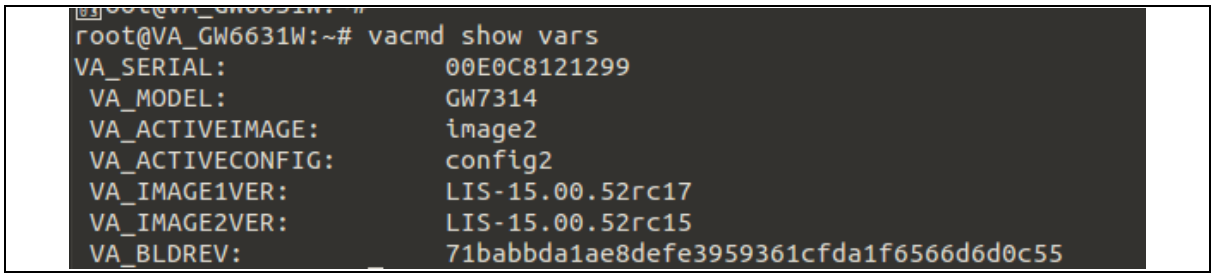


Figure 84: Output from the command vacmd show vars

Alternatively, when you are connected via the web interface, the software version currently being used is presented at the bottom of the screen

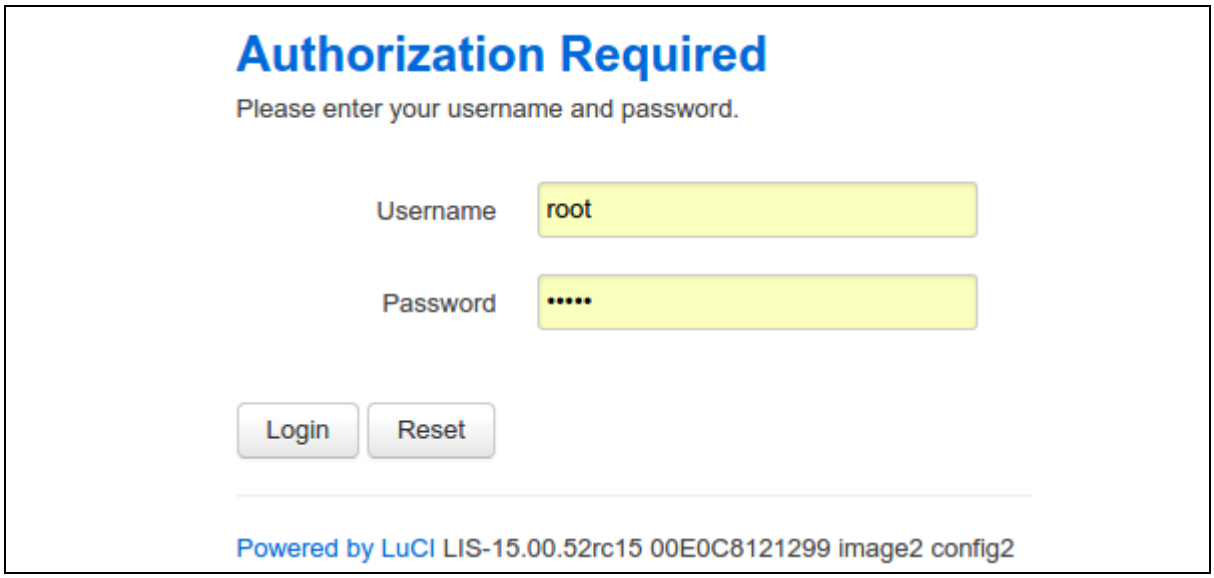


Figure 85: The login screen showing the current software version

24.2 VRRP web interface

To configure VRRP through the web interface, in the top menu, select **Network -> VRRP**. The VRRP page appears.

Figure 86: The VRRP page

In the VRRP page, you can enable or disable VRRP and add, edit or delete VRRP groups.

Under the Global Settings title, click **Add**.

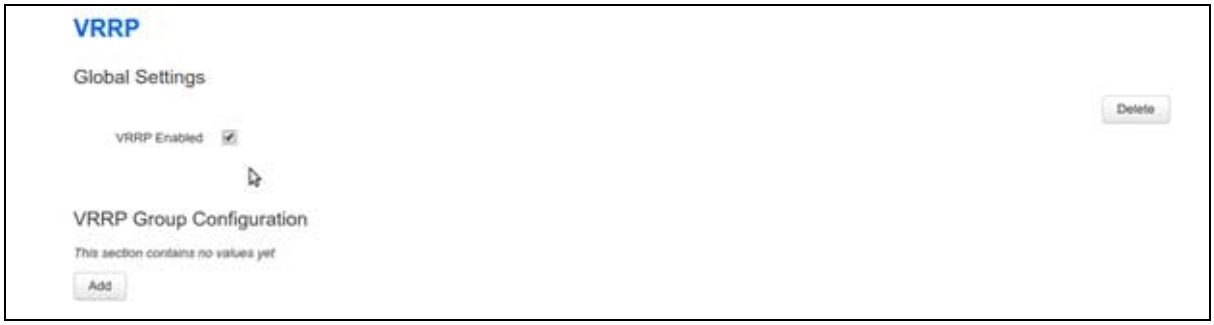


Figure 87: The VRRP global settings section

Check the **VRRP Enabled** checkbox.

Name	Type	Required	Default	Description
VRRP Enabled	Checkbox	yes	Unchecked	Globally enables VRRP on the router.

Under the VRRP Group Configuration title, click **Add**.

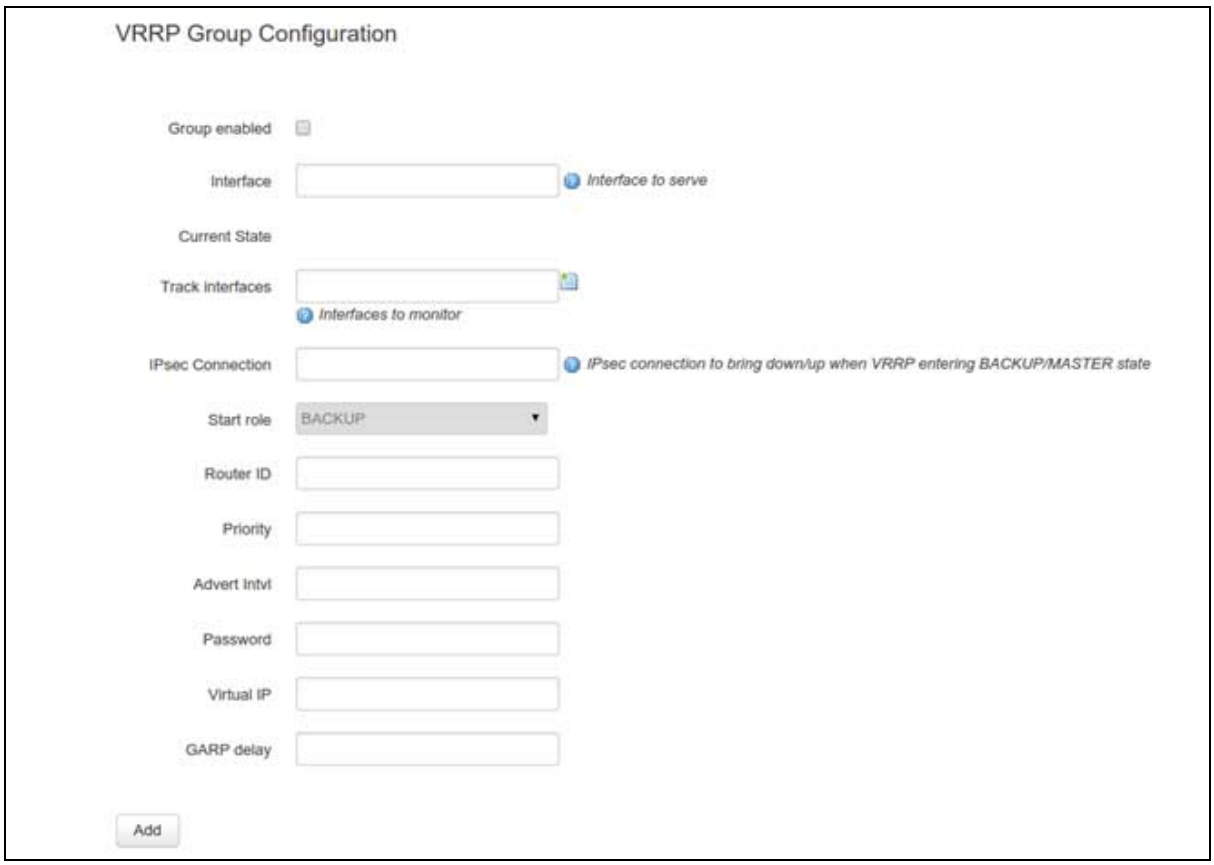


Figure 88: The VRRP group configuration section

Check the **Group enabled** option check box.

In the Interface field, type the name of the interface where VRRP should run.

Note: take the interface name from the interface section.

In the Track interfaces field, optionally provide the name of the interface that should be tracked.

In the Router id field, type the **VRRP ID**.

In the Priority field, set the router's **VRRP priority**.

In the Advert Intvl field, type the **VRRP hello value**.

In the Virtual IP field, provide the **VRRP IP address**.

Click **Save & Apply**.

Name	Type	Required	Default	Description
Group enabled	Checkbox	yes	Unchecked	Enables a VRRP group on the router.
Interface	String	Yes	Blank	Sets the local LAN interface name in which the VRRP cluster is to operate, for example 'lan'.
Track interfaces	List	Yes	Blank	Sets one or more WAN interfaces VRRP should monitor. If a monitored interface goes down on the Master VRRP router, it goes into 'Fault' state and the Backup VRRP router becomes the Master.
IPSec connection	String	No	Blank	Sets which IPSec connection to bring up or down when VRRP enters 'Backup/Master' state.
Start role	Drop down list	Yes	Master	Sets the initial role in which a VRRP router starts up. In a cluster of VRRP routes, set one as a Master and the others as Backup.
Router ID	Integer	Yes	Blank	Sets the VRRP router ID (1 to 255). All co-operating VRRP routers serving the same LAN must be configured with the same router ID.
Priority	Integer	Yes	Blank	Sets the VRRP router's priority. Higher values equal higher priority. The VRRP routers must use priority values between 1-254. The Master router uses a higher priority.
Advert intvl	Integer	Yes	Blank	Sets the VRRP advertisement message sending interface in seconds.
Password	String	No	Blank	Sets the password to use in the VRRP authentication (simple password authentication method). This field may be left blank if no authentication is required.
Virtual IP	String	Yes	Blank	Sets the virtual IP address and mask in prefix format. For example, '11.1.1.99/24'. All co-operating VRRP

				routers serving the same LAN must be configured with the same virtual IP address.
GARP delay	Integer	Yes	Blank	Sets the gratuitous ARP message sending delay in seconds.

Figure 89: The VRRP group configuration fields and their descriptions

24.3 Configuring VRRP using UCI

You can configure VRRP through CLI using UCI commands.

The configuration file is stored at:

/etc/config/vrrp

To view the configuration in UCI format, use the commands:

uci export vrrp

or

uci show vrrp

```
~# uci export vrrp
config vrrp 'main'
        option enabled 'yes'

config vrrp_group 'g1'
        option enabled 'yes'
        option interface 'lan1'
        list track_iface 'lan'
        option init_state 'BACKUP'
        option router_id '1'
        option priority '115'
        option advert_int_sec '2'
        option password 'secret'
        option virtual_ipaddr '10.1.10.150/16'
        option garp_delay_sec '5'
       option ipsec_connection 'Test'
```

```
~# uci show vrrp
vrrp.main=vrrp
vrrp.main.enabled=yes
vrrp.g1=vrrp_group
vrrp.g1.enabled=yes
vrrp.g1.interface=lan1
vrrp.g1.track_iface=lan
vrrp.g1.init_state=BACKUP
vrrp.g1.router_id=1
vrrp.g1.priority=115
vrrp.g1.advert_int_sec=2
vrrp.g1.password=secret
vrrp.g1.virtual_ipaddr=10.1.10.150/16
vrrp.g1.garp_delay_sec=5
vrrp.g1.ipsec_connection=Test
```

Name	Type	Required	Default	Description
enabled		yes	Blank	Enables VRRP
vrrp_group	Text	Yes	Blank	VRRP GROUP ID number
enabled		yes	Blank	Enables VRRP Group
interface	text	yes	Blank	Interface name where VRRP should run. Interface name taken from package network
track_iface	text	yes	Blank	Interface name that should be tracked/monitored
init_state	text	Yes	BACKUP	Initial VRRP state
priority	Numeric value	yes	Blank	VRRP Priority number. Available values 0-255
advert_int_sec	Numeric value	yes	Blank	VRRP hello value. This value needs to match what is set on a peer.
password	Text	No	Blank	VRRP clear text password
virtual_ipaddr	IP address	Yes	Blank	VRRP IP address
garp_delay_sec	Numeric value	No	Blank	Delay for gratuitous ARP messages
ipsec_connection				
Ipsec connection	text	yes	Blank	IPsec connection name to bring down/up when VRRP entering BACKUP/MASTER state

Table 2: Config interface fields and their descriptions

To change any of the above values use uci set command.

25 Dial modem

Virtual Access GW6630 Series routers are optionally fitted with a V.90 modem.

The table below shows standards that are supported.

Data modem	V.90 V.34 V.32bis V.32 V.29 V.22bis V.22 V.22 Fast Connect V.23 V.21 Bell212a Bell103
Data compression	V.44 V.42bis and MNP5 V.42 LAPM and MNP2-4 error correction

Table 11: Dial modem standards

25.1 V.90 modem scenarios

You can use the V.90 modem in several scenarios. The table below gives a brief description of these scenarios, while the following sections describe how to set up and configure the modem.

Scenario	Description
As a normal WAN interface	Use the V.90 modem in the same way as other WAN interfaces such as DSL and ISDN.
As a backup WAN interface	Set up the V.90 modem to come into operation if the primary WAN interface becomes unusable for some reason.
As an out-of-band management interface	Use the V.90 modem to access the router management functions by dialling into the router, for example, using Virtual Access Router. It is also possible for the router to dial out via the V.90 modem interface under some conditions.

Table 12: V.90 modem scenarios

25.2 Setting up the V.90 physical port connection

To set up the physical modem interface, connect one end of your modem cable to your phone line wall socket and the other end to the RJ-45 modem port.

© Virtual Access 2015

Figure 90: The GW6630 Series router showing physical port connection

25.3 Configuring the modem as a dial out interface via UCI interface

To allow the router to use the PSTN modem to make outbound calls, you must configure a dial out interface.

The dial out configuration files are stored on:

Network files /etc/econf/network

```
uci export network
config interface 'dialout5'
        option proto 'ppp'
        option auto '0'
        option device '/dev/ttyCX0'
        option noipdefault '1'
        option peerdns '0'
        option nopersist '1'
        option defaultroute '0'
        option pppd_options '19200  lcp-echo-interval 10'
        option username 'test'
        option password 'test1'
        option number '1234'
```

To view UCI commands, use the following commands:

```
uci show network
network.dialout5=interface
network.dialout5.proto=ppp
network.dialout5.auto=0
network.dialout5.device=/dev/ttyCX0
network.dialout5.noipdefault=1
network.dialout5.peerdns=0
network.dialout5.nopersist=1
network.dialout5.defaultroute=0
```

```
network.dialout5.pppd_options=19200  lcp-echo-interval 10
network.dialout5.username=test
network.dialout5.password=test1
network.dialout5.number=1234
```

25.4 Configuring the modem as a dial in interface via UCI

To allow out of band management access to the router using the PSTN modem, you must configure three settings.

- **Mgetty**: assigns the inbound call to the modem.
- **Dial in interface**: assigns and establishes a PPP connection.
- **Management user**: for control of a secure connection.

25.4.1 Mgetty settings

The configuration files are stored on:

Mgetty files /etc/config/mgetty

```
uci export mgetty
package mgetty
config mgetty 'main'
        option enabled 'yes'

config device 'ttyCX0'
        option device '/dev/ttyCX0'
        option ppp_iface 'dialin'
        option login_user 'test'
        option init_chat '"" \d+++\dAT&F+VCID=1 OK'
        option answer_chat '"" ATA CONNECT 38400'
        option data_only '1'
        option rings '1'
        option speed '9600'
        option debug '9'
```

To view the configuration files, enter:

```
uci show mgetty
mgetty.main=mgetty
```

```
mgetty.main.enabled=yes
mgetty.ttyCX0=device
mgetty.ttyCX0.device=/dev/ttyCX0mgetty.ttyCX0.ppp_iface=dialin
mgetty.ttyCX0.init_chat="" \d+++\dAT&F+VCID=1 OK
mgetty.ttyCX0.answer_chat="" ATA CONNECT 19200
mgetty.ttyCX0.data_only=1
mgetty.ttyCX0.rings=2
mgetty.ttyCX0.speed=19200
mgetty.ttyCX0.debug=9
```

25.4.2 Dial in interface settings

The configuration files are stored on:

Network files /etc/config/network

```
uci export network
config interface 'dialin'
        option proto 'ppp'
        option auto '0'
        option peerdns '1'
        option remote_ipaddr '172.168.101.2'
        option local_ipaddr '172.168.101.1'
        option noipdefault '1'
        option defaultroute '0'
        option remote_auth_options 'require_eap'
```

To view the configuration files, enter:

```
uci show network
network.dialin=interface
network.dialin.proto=ppp
network.dialin.auto=0
network.dialin.peerdns=1
network.dialin.remote_ipaddr=172.168.101.2
network.dialin.local_ipaddr=172.168.101.1
network.dialin.noipdefault=1
```

```
network.dialin.defaultroute=0
network.dialin.remote_auth_options=require_eap
```

25.4.3 Management user settings

The configuration files are stored on:

Management user files /etc/config/managerment_user

```
uci export managment_users
package managment_users
config user
        option enabled '1'
        option username 'test'
        option password 'test'
        option srpuser '1'
        option chapuser '0'
        option webuser '0'
        option smsuser '0'
        option linuxuser '0'
```

To view the configuration files, enter:

```
uci show managment_users
managment_users.@user[0]=user
managment_users.@user[0].enabled=1
managment_users.@user[0].username=test
managment_users.@user[0].password=test
managment_users.@user[0].srpuser=1
managment_users.@user[0].chapuser=0
managment_users.@user[0].webuser=0
managment_users.@user[0].smsuser=0
managment_users.@user[0].linuxuser=0
```

© Virtual Access 2015

26 ISDN pseudowire

26.1 Introduction

ISDN pseudowire is delivered via an ISDN S/T interface in NT mode. This allows you to connect existing ISDN equipment with BRI interfaces, such as phones, audio contribution boxes, and so on, directly to the Virtual Access router.

When the ISDN equipment attempts to make a call, its messages are converted into SIP/RTP protocol and relayed to a provider, such as the GW7610-PRI. The GW7610-PRI is connected directly to a real ISDN network and converts the messages received over SIP/RTP back into native ISDN messages for the real ISDN network.

In this way, access to the real ISDN network is extended to the remote site over IP and the equipment at the remote site that is connected to GW6610-ISDN will be able to make and receive calls to and from any number on the real network.

The router is equipped with an ADSL WAN interface and is the interface of choice for connecting the device to the core network.

Note: success of the pseudowire relies on the network's ability to transfer the data without loss between the Virtual Access router and the provider. IP packet loss will result in momentary corruption of data, typically around 20 milliseconds in length. If you apply a codec to the data content, the codec may need to resynchronise the data stream, resulting in a larger outage of length determined solely by the codec.

When configuring ISDN Pseudowire, you must decide the device's role. A device typically acts as a client, which is the usual role for a GW6610-ISDN; provider, which is the usual role for GW7610-PRI; or both, which is the usual role for GW6610-ISDN in a back-to-back scenario.

The following sections explain the configuration of two scenarios using a GW6610-ISDN as an example.

- GW6610-ISDN in client role
    - This allows ISDN user equipment connected to the GW6610-ISDN unit to reach, or be reached from any number on the ISDN network available at the provider, typically a GW7610-PRI.
- GW6610-ISDN in client and provider role
    - This allows ISDN user equipment connected to the GW6610-ISDN unit on one site connect to ISDN user equipment at another site, where there is another GW6610-ISDN unit.

26.2 Pseudowire functionality

Two packages are used to control the ISDN to SIP/RTP conversion.

These packages are **Asterisk** and **LCR** (Linux Call Router).

LCR acts as a channel driver and allows asterisk to access the ISDN hardware. **Asterisk** then sends SIP messages to the provider to establish communications channels and forwards the data content of active ISDN B channels over RTP.

The router has an automatic clock recovery feature to allow the BRI interface to effectively run at the same clock rate as the provider.

26.3 ISDN pseudowire in client role

The most typical scenario for the GW6610-ISDN is for it to act in a client role whereby locally attached ISDN equipment can make and receive calls on a remote ISDN network over an IP network, typically via the ADSL interface on the GW6610-ISDN router.

In the example below it is assumed the routers involved have the following attributes:

- GW6610-ISDN client has two MSNs (Multiple Subscriber Numbers): 384720 and 384721
- A provider exists at 10.1.23.15

26.3.1 Configuring LCR using UCI

You only need to configure LCR with the MSN of the user equipment connected to the BRI interface on the router. Most ISDN user equipment supports two or more MSNs.

LCR configuration files are stored at: **/etc/config/lcr**

```
root@VA_router:~# uci export lcr
package lcr

config lcr 'main'
        option enable '1'
        list msn '384720'
        list msn '384721'
```

The following tables describe the UCI parameters for each section.

config lcr 'main'

Name	Required	Default	Description
Enable	Yes	1	Specifies whether or not LRC should run and allow asterisk access to the ISDN hardware.
msn	Yes		Specifies the MSN number that the ISDN user equipment is configured to respond to. You can configure multiple MSN's as list entries.

26.3.2 Configuring Asterisk using UCI

You must configure Asterisk with an identifying address, to enable it to reach the provider and credentials.

Asterisk configuration files are stored at: **/etc/config/asterisk**

```
root@VA_router:~# uci export asterisk
package asterisk

config provider
        option host '10.1.23.15'
        option hostport '5060'
        option username 'usernameForUnit20'
        option secret 'secretForUnit20'
```

The following tables describe the UCI parameters for each section.

config provider

Name	Required	Default	Description
host	Yes		Specifies the IP address of the provider to register with.
hostport	No	5060	Specifies the port to send registration requests to.
username	Yes		Specifies the username to present to the provider to identify this site. Note: The provider will be configured with an association for this username and an MSN hosted by this unit. Calls to MSN's configured on this site will only be routed to this site if the provider is configured with the appropriate username/password/MSN triplet.
password	Yes		Specifies the password to present to the provider to identify this site.

26.4 ISDN pseudowire in client and provider role (back-to-back)

Another scenario is to use two routers to connect two sites so that they can make and receive ISDN between one another over IP. As the entire network is self-contained, you can choose any numbering plan and it does not need to agree with 'real-world' numbering.

In the example below it is assumed the routers involved have the following attributes. Typically this scenario would be implemented using two GW6610-ISDN routers.

- First GW6610-ISDN client
  - has two MSNs: 384720 and 384721
  - exists at address 10.1.183.20
- Second GW6610-ISDN client
  - has two MSNs 384740 and 384741
  - exists at address 10.1.183.40

26.4.1 Configuring LCR using UCI

You only need to connect LCR with the MSNs of the user equipment connected to the BRI interface on the router. Most ISDN user equipment supports two or more MSNs.

LCR configuration files are stored at: **/etc/config/lcr**

```
root@VA_router:~# uci export lcr
package lcr

config lcr 'main'
        option enable '1'
        list msn '384720'
        list msn '384721'
```

config lcr 'main'

Name	Required	Default	Description
Enable	Yes	1	Specifies whether or not LRC should run and allow asterisk access to the ISDN hardware.
msn	Yes		Specifies the MSN number that the ISDN user equipment is configured to respond to. You can configure multiple MSN's as list entries.

26.4.2 Configuring Asterisk using UCI

You must configure Asterisk with an identifying address, to enable it to reach the provider and credentials.

In addition you must configure details of the remote ISDN equipment that is connecting to this router using the config client options

Asterisk configuration files are stored at: **/etc/config/asterisk**

```
root@VA_router:~# uci export asterisk
package asterisk

config provider
        option host '10.1.183.40'
        option hostport '5060'
        option username 'usernameForUnit20'
        option secret 'secretForUnit20'

config client
        option username 'usernameForUnit40'
        option secret 'secretForUnit40'
        option msn '384740'

config client
        option username 'usernameForUnit40' #typically same as above
        option secret 'secretForUnit40’ #typically same as above
        option msn '384741'
```

config provider

Name	Required	Default	Description
host	Yes		Specifies the IP address of the provider to register with.
hostport	No	5060	Specifies the port to send registration requests to.
username	Yes		Specifies the username to present to the provider to identify this site. Note: The provider will be configured with an association for this username and an MSN hosted by this unit. Calls to MSN's configured on this site will only be routed to this site if the provider is configured with the appropriate username/password/MSN triplet.
password	Yes		Specifies the password to present to the provider to identify this site.

Note: the configuration for the provider in back-to-back mode is identical to that for client only mode. This is because, as in client mode, the unit must simply register with a provider and prove its identity.

To complete the configuration, the settings must also allow the other GW6610-ISDN unit in the back-to-back pair to connect to this unit. To do so, one ‘client’ section is required for each MSN number hosted by the other GW6610-ISDN unit. As most ISDN equipment supports at least two MSN numbers, there are typically two or more such sections.

Name	Type	Required	Default	Description
username	Text	Yes		Specifies a username to accept from the other party to identify themselves.
password	Text	Yes		Specifies the password to accept from the other party identifying themselves with the username.
msn	Numeric	Yes		Specify the MSN numbers to route to this other party when a call is received (from the BRI interface).

Note: on the other device there will also be an LCR configuration and an Asterisk configuration where the provider and client sections are swapped.

A typical example of an asterisk and LCR configuration for the other unit in a back-to-back configuration is shown below.

```
root@VA_router:~# uci export lcr
package lcr

config lcr 'main'
        option enable '1'
        list msn '384740'
        list msn '384741'

~# uci export asterisk
package asterisk

config provider
        option host '10.1.183.20'
        option hostport '5060'
        option username 'usernameForUnit40'
        option secret 'secretForUnit40'
```

```
config client
        option username 'usernameForUnit20'
        option secret 'secretForUnit20'
        option msn '384720'

config client
        option username 'usernameForUnit20' #typically same as above
        option secret 'secretForUnit20' #typically same as above
        option msn '384721'
```

27 Analogue Leased Line interface

The Analogue Leased Line (ALL) interface provides a 2- or 4-wire analogue interface. The behaviour of the interface depends on the application using it. The interface can currently be used with two applications: Terminal Server or CESoPSN.

The ALL interface has the device name ‘ttyLC0’.

27.1 Terminal Server: V.23 modem emulation

When used with the Terminal Server application the ALL interface enables a V.23 modem emulation. The V.23 modem emulation passes the decoded modem call data to the terminal server application.

Note: gain and attenuation cannot currently be controlled when operating in V.23 modem emulation mode.

27.2 CESoPSN: transparent mode

When used with CESoPSN the PCM encoded data is passed transparently to the application which then encapsulates in CESoPSN data packets.

27.3 Gain and attenuation control

The ALL interface provides you with the possibility to adjust the gain and attenuation. The diagram below shows the signal flow and the options available to control it.

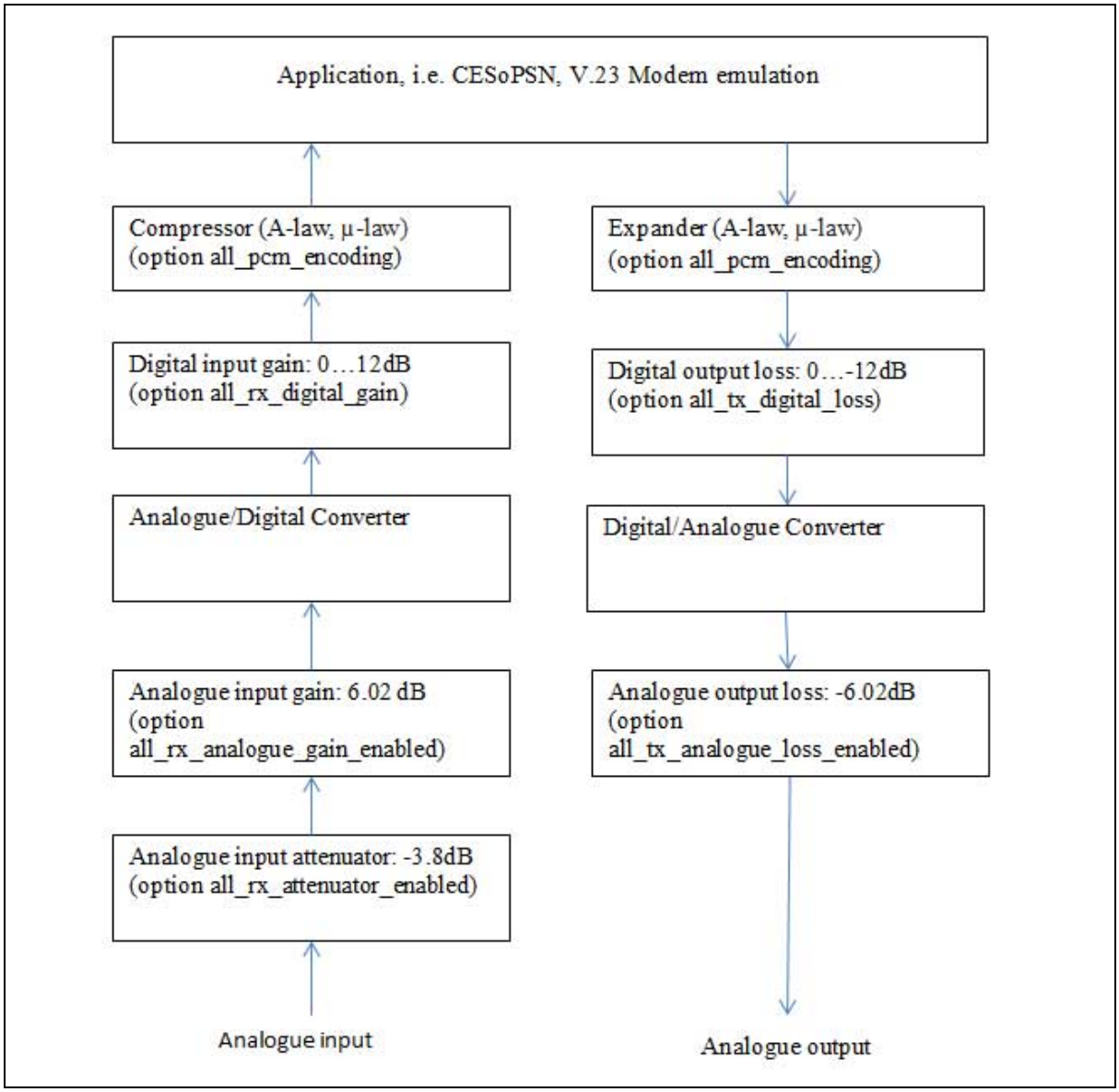


Figure 91: Gain and attenuation flow

27.4 ALL interface

The ALL interface has the device name **'ttyLC0'**.

27.4.1 ALL status

To view the status of the ALL interface, enter:

```
va5420_status /dev/ttyLC0
```

```
root@client_B:~#
root@client_B:~# va5420_status /dev/ttyLC0
Mode:           Transparent
Wire mode:      2-wire
PCM Encoding:   A-Law
root@client_B:~#
```

27.4.2 ALL statistics

To view statistical information about the ALL interface, enter `va5420_stats /dev/ttyLC0`.

```
root@VA_router:~# va5420_stats /dev/ttyLC0
TRANSMIT STATS
      tx bytes                 44661000
      tx buffer full counts    0
      tx underruns             289
      tx discards              16280

RECEIVE STATS
      rx bytes                 44692864
      rx overruns              33
      rx discards              0
```

Tx underruns or discards can indicate that there is no jitter buffer enabled in the CESoP configuration.

Note: enabling a jitter buffer will add latency.

To see whether a jitter buffer is enabled, enter:

```
root@VA_router:~# # uci export cesopd

package cesopd

config cesopd 'main'
        option log_severity '5'
        option enable '1'

config port 'Port1'
        …..
        option rx_jitter_buffer_enabled ‘1’
```

27.4.3 ALL wiring

2-wire

RJ-11		RJ-45
2 RED (TIP)	-	5 tx/rx

3 GREEN (RING)	-	4 tx/rx

4-wire

RJ-11		RJ-45
1 YELLOW (TIP1)	-	5 TIP1
2 RED (TIP)	-	6 TIP
3 GREEN (RING)	-	3 RING
4 BLACK (RING1)	-	4 RING1

RJ45 SMG

1 not connected

2 not connected

3 RX

4 TX

5 TX

6 RX

7 Not connected

8 not connected

28 Configuring CESoPSN

28.1 What is CESoPSN?

CESoPSN (Circuit Emulation Services over Packet Switched Network) is a mechanism for transporting Time Division Multiplexing (TDM) signals over Packet-Switching Networks (PSNs). CESoPSN is specified in RFC5086.

CESoPSN is currently supported on router models fitted with an Analogue Leased Line (ALL) or Dual X.21 module.

CESoPSN and clock recovery

Router models supporting CESoPSN have a variable TDM clock allowing it to synchronize with the TDM clock of its peer. For the CESoPSN function to work satisfactory it is essential that you synchronize the internal clocks for generating the TDM signals of the routers. That is, run at exactly the same frequency, otherwise over- and under-runs in the packet buffers will occur.

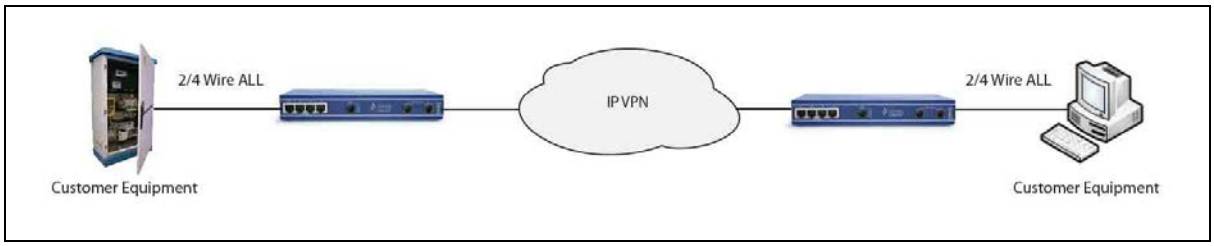


Figure 92: CESoPSN architecture

Note: Ensure you enable clock recovery on the clock slave **only**.

28.2 Configuring CESoPSN using UCIJK

The CESoPSN configuration file is stored at: **/etc/config/cesopd**

28.2.1 Main settings

The main settings are stored in the cesopd section of /etc/config/cesopd. There is only one cesopd section.

```
config cesopd 'main'
        option log_severity '5'
        option enable '1'
```

Name	Type	Required	Default	Description
enable	boolean yes|no	Yes	no	Yes: enables CESoPSN services. No: disables CESoPSN services.

log_severity	Integer 0…7	No	5	Selects the severity used for logging events CESoPSN in syslog. The following levels are available: 0 - Emergency 1 - Alert 2 - Critical 3 - Error 4 - Warning 5 - Notice 6 - Informational 7 - Debug

28.3 Port settings

Settings for the individual ports are stored in the port sections of /etc/config/cesopd. Each port has its own section. A maximum of 2 ports are supported.

The example below shows a port section labelled ‘Port 1’.

```
config port 'Port1'
        option enable '1'
        option devname 'ttyLC0'
        option udp_local_ipaddr '0.0.0.0'
        option udp_remote_ipaddr '10.1.42.63'
        option udp_local_port '5152'
        option udp_remote_port '5152'
        option rtp_payload_type '96'
        option rx_jitter_buffer_size_ms '24'
        option rate '64000'
        option clock_recovery_enabled '1'
        option packetization_latency '5'
        …….
        <port config also contains port specific options>
```

Name	Type	Required	Default	Description
enable	boolean	Yes	0	Enables the port.
devname	String	Yes	ttyXHFC0	Selects the serial interface to be used with this port. ‘ttyLC0’: ALL interface ‘ttyXHFC0’: first Dual X.21 port ‘ttyXHFC1’:second Dual X.21 port

udp_local_ipaddr	IP Address	Yes	'127.0.0.1'	Specifies the interface IP address to listen on for incoming packets. '0.0.0.0' means listen on all available interfaces.
udp_remote_ipaddr	IP Address	Yes	'127.0.0.1'	Specifies the remote IP address to send packets to. If the remote address is '0.0.0.0' packets are accepted from all sources and received source IP address will be used as destination.
udp_local_port	Integer 0…65535 (49152…65535 recommended)	Yes	5566	UDP port to listen for incoming packets on.
udp_remote_port	Integer 0…65535 (49152…65535 recommended)	Yes	6655	UDP port to send packets to. Port can be 0. In that case the source port of the incoming packets will be used as the destination.
rtp_payload_type	Integer 0…127	No	96	Specifies the RTP payload header type. Default is 96 (Dynamic). RTP payload types are specified by IANA (Internet Assigned Numbers Authority); see http://www.iana.org/assignments/rtp-parameters/rtp-parameters.txt for the complete range of available types.
clock_recovery_enabled	boolean	No	0	If enabled, this port will use the received packet data to adjust the TDM data clock of the router. Note: enable clock recovery on one port only.
rx_jitter_buffer_enabled	boolean	No	0	Enables/disables the network jitter buffer.
rx_jitter_buffer_size_ms	Integer 0…160	No	16	Defines the size of the network jitter buffer.
packetization_latency	Integer 5…20	No	8	Specifies the packetization latency in milliseconds.
rate	Integer 64000…2048000	Yes	64000	Selects the interface rate. The rate has to be a multiple of 64000. For the ALL interface only 64000 is supported.

Interface specific port settings are described in the following sub-chapters.

28.3.1 ALL interface settings

```
config port 'Port1'
        option enable '1'
        option devname 'ttyLC0'
        …….
        <generic port options>
        …….
        option all_four_wire_mode '0'
        option all_pcm_encoding 'alaw'
        option all_tx_analogue_loss_enabled '1'
        option all_tx_digital_loss '6'
        option all_rx_analogue_gain_enabled '1'
        option all_rx_digital_gain '2'
        option all_rx_attenuator_enabled '1'
```

Name	Type	Required	Default	Description
all_four_wire_mode	Boolean	No	0	If set to '1' the ALL interfaces operates in 4-wire mode, otherwise in 2-wire mode (default).
all_pcm_encoding	String 'alaw'| 'ulaw'	No	'alaw'	Selects the PCM companding algorithm. 'alaw' – selects the A-law algorithm 'ulaw' – selects the µ-law algorithm. For more details see ITU-T G.711.
all_tx_digital_loss	Integer 0…12	No	0	Specifies the output digital loss (attenuation) in dB.
all_rx_digital_gain	Integer 0…12	No	0	Specifies the input digital gain in dB.
all_rx_analogue_gain_enabled	Boolean	No	0	Enables an analogue 6.02dB input gain
all_tx_analogue_loss_enabled	Boolean	No	0	Enables an analogue 6.02dB output loss (attenuation)
all_rx_attenuator_enabled	Boolean	No	1	Enables the analogue input attenuator (3.8dB)

28.3.2 Dual X.21 interface settings

Not currently available.

29 Dynamic Multipoint Virtual Private Network (DMVPN)

Dynamic Multipoint Virtual Private Network (DMVPN) is a scalable method of creating VPN IPSec Networks. DMVPN is a suite of three protocols: NHRP, mGRE and IPSec, used to dynamically create VPN tunnels between different endpoints in the network without having to pre-configure each device with VPN details of the rest of endpoints in the network.

29.1 The advantage of using DMVPN

- Using DMVPN eliminates the need of IPSec configuration to the physical interface. This reduces the number of lines of configuration required for a VPN development. For example, for a 1000-site deployment, DMVPN reduces the configuration effort at the HUB from 3900 lines to 13.
- Adding new peers (spokes) to the VPN requires no changes at the HUB.
- Better scalability of the network.
- Dynamic IP addresses can be used at the peers' site.
- Spokes can be connected in private or public network.
- NHRP NAT extension allows spoke-to-spoke tunnels to be built, even if one or more spokes is behind a Network Address Translation (NAT) device.
- New HUBs can be added to the network to improve the performances and reliability.
- Ability to carry multicast and main routing protocols traffic (RIP, OSPF, BGP).
- DMVPN can be deployed using Activator, the Virtual Access automated provisioning system.
- Simplifies branch communications by enabling direct branch to branch connectivity.
- Simplifies configuration on the spoke routers. The same IPSec template configuration is used to create spoke-to-hub and spoke-to-spoke VPN IPSec tunnel.
- Improves business resiliency by preventing disruption of business-critical applications and services by incorporating routing with standards-based IPsec technology.

29.2 DMVPN scenarios

Scenario 1: Spoke1, Spoke2 and a hub are in the same public or private network

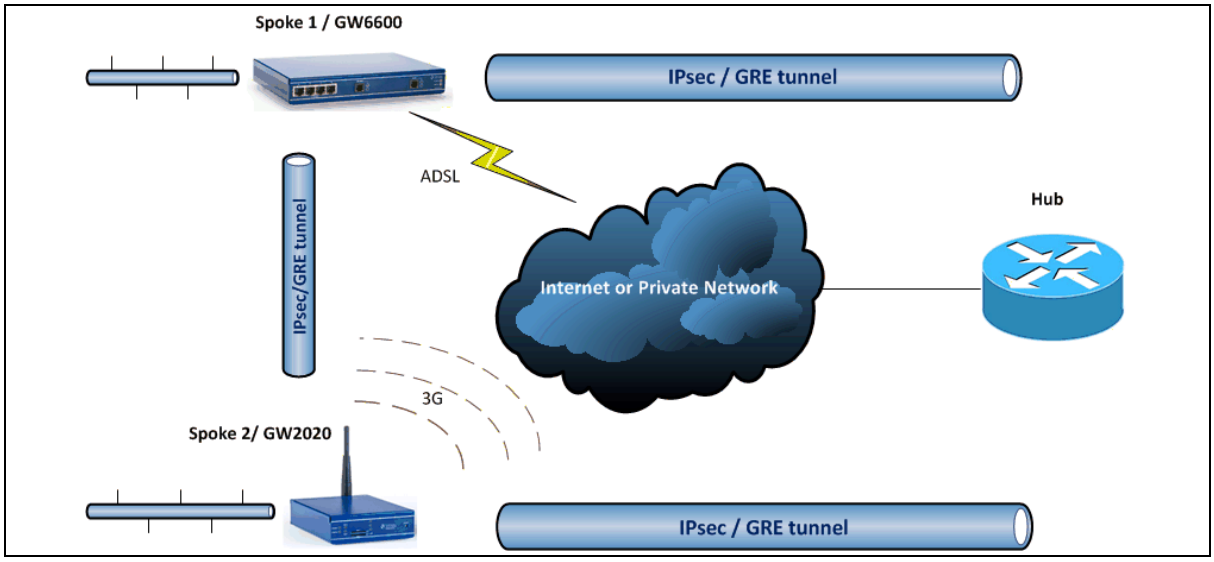


Figure 93: Network diagram for DMVPN spoke to spoke

- Spoke1 and Spoke2 connect on their WAN interface: ADSL, 3G and initiate main mode IPSec in transport mode to the hub.
- After an IPSec tunnel is established, spokes register their NHRP membership with the hub.
- GRE tunnels come up.
- Hub cache the GRE tunnel and real IP addresses of each spoke.
- When Spoke1 wants to talk to Spoke2, it sends an NHRP Resolution Request to the hub.
- The hub checks its cache table and forwards that request to Spoke2.
- Spoke2 caches Spoke1's GRE and real IP address and sends an NHRP Resolution Reply via the hub.
- Spoke1 receives an NHRP resolution reply and updates its NHRP table with Spoke2 information. Then it initiates VPN IPsec connection to Spoke2.
- When an IPsec tunnel is established, Spoke1 and Spoke2 can send traffic directly to each other.

Scenario 2: Spoke1 is in a private (NAT-ed) network, Spoke2 and hub are in public network

© Virtual Access 2015

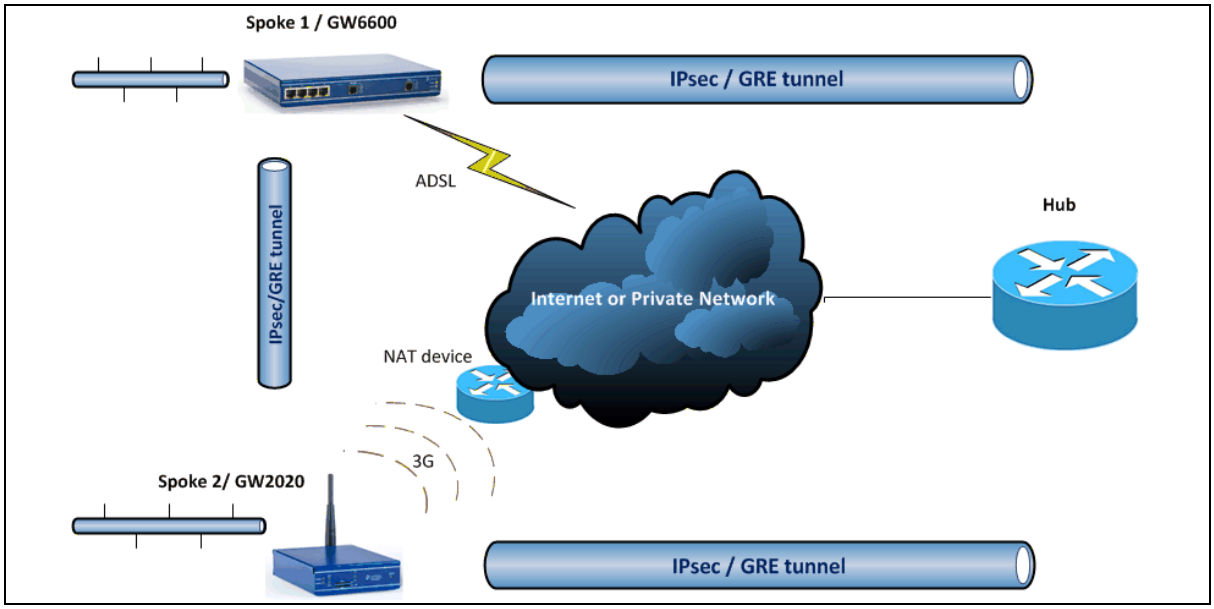


Figure 94: Network diagram for DMVPN spoke behind NAT

- Spoke1 sends an NHRP registration request to the Hub.
- Hub receives this request and compares the source tunnel address of the Spoke with the source of the packet.
- Hub sends an NHRP registration reply with a NAT extension to Spoke1.
- The NAT extension informs Spoke1 that it is behind the NAT-ed device.
- Spoke1 registers its pre- and post-NAT address.
- When Spoke1 wants to talk to Spoke2, it sends an NHRP Resolution Request to the hub.
- Hub checks its cache table and forwards that request to Spoke2.
- Spoke2 caches Spoke1's GRE pre- and post-NAT IP address and sends an NHRP Resolution Reply via the hub.
- Spoke1 receives the NHRP resolution reply and updates its NHRP table with Spoke2 information. It initiates a VPN IPSec connection to Spoke2.
- When the IPSec tunnel is established, Spoke1 and Spoke2 can send traffic directly to each other.
- Note: If an IPSec tunnel fails to be established between the Spokes then packets between the Spokes are sent via the hub.

29.3 Configuring DMVPN via the web interface

Before configuring DMVPN, you must first configure a GRE interface. Read the previous section,'GRE interfaces'.

29.3.1 Configuring IPSec for DMVPN

This section explains how to configure VPN IPSec specifically for DMVPN. For more information on general VPN IPSec configuration, read 'Configuring IPSec' in the GW6600 User Manual.

Access the router's web Interface by typing 192.168.100.1 into your browser.

Type in the username: **root**

Type in the password: **admin**. The Status page appears.

In the top menu click **Services -> IPSec**. The strongSwan IPSec VPN page appears.

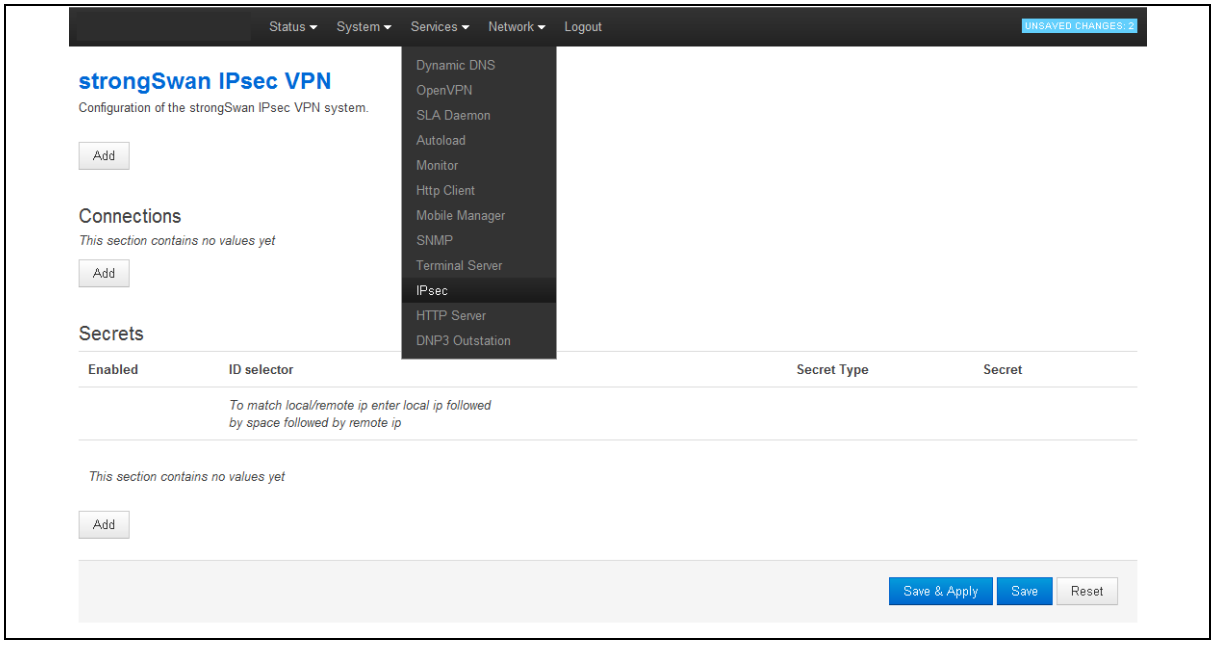


Figure 95: The strongSwan IPSec VPN page

Click the first **Add** button. The strongSwan status now shows an Enabled field that is checked.

strongSwan IPsec VPN
Configuration of the strongSwan IPsec VPN system.
Delete
Enable StrongSwan IPsec
Strict CRL Policy
no
Defines if a fresh CRL must be available in order for the peer authentication based on RSA signatures to succeed. IKEv2 additionally recognizes 'ifuri' which reverts to 'yes' if at least one CRL URI is defined and to 'no' if no URI is known.
Unique IDs
yes
Whether a particular participant ID should be kept unique, with any new (automatically keyed) connection using an ID from a different IP address deemed to replace all old ones using that ID. Participant IDs normally are unique, so a new (automatically-keyed) connection using the same ID is almost invariably intended to replace an old one. The IKEv2 daemon also accepts the value 'replace' which is identical to 'yes' and the value 'keep' to reject new IKE SA setups and keep the duplicate established earlier.
Cache CRLs
CRLs fetched via HTTP or LDAP will be cached.
Debug
none
Connections
This section contains no values yet
Add

Figure 96: strongSwan IPSec enabled

Name	Type	Required	Default	Description
Enable Strongswan IPsec	Boolean	Yes	Blank	Enable Strongswan IPsec
Strict CRL Policy	Dropdown menu	Yes	No	Defines if fresh certificate revocation list (CRL) must be available.
Unique IDs	Dropdown menu	Yes	Yes	Whether a particular participant ID should be kept unique.
Cache CRLs	Boolean	No	Blank	CRLs fetched via HTTP or LDAP will be cached.
Debug	Dropdown menu	No	None	Specifies if IPsec debug should be enabled

Table 13: strongSwan IPSec VPN fields and their descriptions

In the Unique IDs drop down menu, select **Yes**. The Connections settings fields appear.

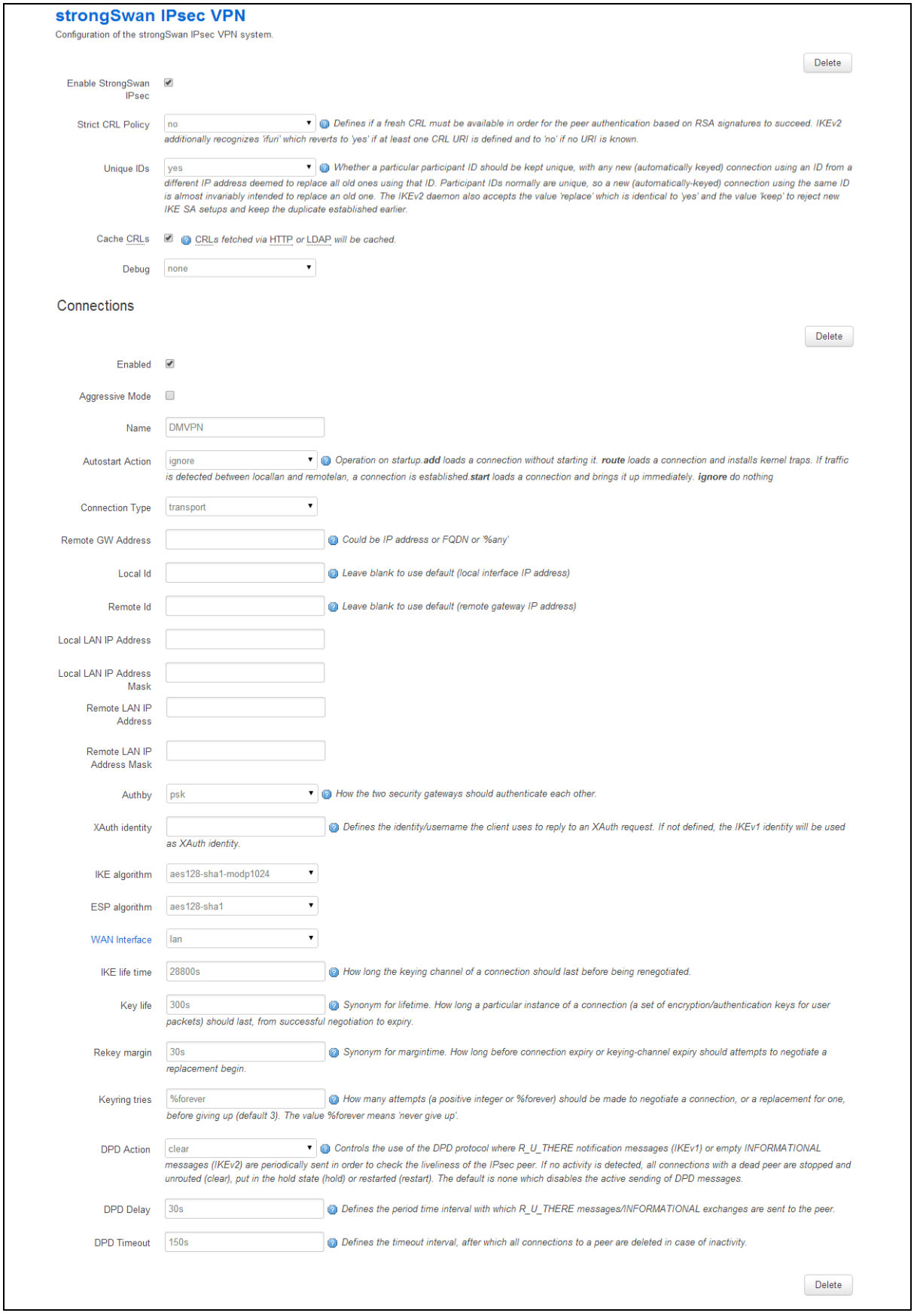

strongSwan IPsec VPN
Configuration of the strongSwan IPsec VPN system.
Delete
Enable StrongSwan IPsec
Strict CRL Policy
no
Defines if a fresh CRL must be available in order for the peer authentication based on RSA signatures to succeed. IKEv2 additionally recognizes 'ifuri' which reverts to 'yes' if at least one CRL URI is defined and to 'no' if no URI is known.
Unique IDs
yes
Whether a particular participant ID should be kept unique, with any new (automatically keyed) connection using an ID from a different IP address deemed to replace all old ones using that ID. Participant IDs normally are unique, so a new (automatically-keyed) connection using the same ID is almost invariably intended to replace an old one. The IKEv2 daemon also accepts the value 'replace' which is identical to 'yes' and the value 'keep' to reject new IKE SA setups and keep the duplicate established earlier.
Cache CRLs
CRLs fetched via HTTP or LDAP will be cached.
Debug
none
Connections
Delete
Enabled
Aggressive Mode
Name
DMVPN
Autostart Action
ignore
Operation on startup.add loads a connection without starting it. route loads a connection and installs kernel traps. If traffic is detected between locallan and remotelan, a connection is established.start loads a connection and brings it up immediately. ignore do nothing
Connection Type
transport
Remote GW Address
Could be IP address or FQDN or '%any'
Local Id
Leave blank to use default (local interface IP address)
Remote Id
Leave blank to use default (remote gateway IP address)
Local LAN IP Address
Local LAN IP Address Mask
Remote LAN IP Address
Remote LAN IP Address Mask
Authby
psk
How the two security gateways should authenticate each other.
XAuth identity
Defines the identity/username the client uses to reply to an XAuth request. If not defined, the IKEv1 identity will be used as XAuth identity.
IKE algorithm
aes128-sha1-modp1024
ESP algorithm
aes128-sha1
WAN Interface
lan
IKE life time
28800s
How long the keying channel of a connection should last before being renegotiated.
Key life
300s
Synonym for lifetime. How long a particular instance of a connection (a set of encryption/authentication keys for user packets) should last, from successful negotiation to expiry.
Rekey margin
30s
Synonym for margintime. How long before connection expiry or keying-channel expiry should attempts to negotiate a replacement begin.
Keyring tries
%forever
How many attempts (a positive integer or %forever) should be made to negotiate a connection, or a replacement for one, before giving up (default 3). The value %forever means 'never give up'.
DPD Action
clear
Controls the use of the DPD protocol where R_U_THERE notification messages (IKEv1) or empty INFORMATIONAL messages (IKEv2) are periodically sent in order to check the liveliness of the IPsec peer. If no activity is detected, all connections with a dead peer are stopped and unrouted (clear), put in the hold state (hold) or restarted (restart). The default is none which disables the active sending of DPD messages.
DPD Delay
30s
Defines the period time interval with which R_U_THERE messages/INFORMATIONAL exchanges are sent to the peer.
DPD Timeout
150s
Defines the timeout interval, after which all connections to a peer are deleted in case of inactivity.
Delete

Figure 97: The strongSwan IPSec VPN page

Name	Type	Required	Default	Description
Enabled	Checkbox	yes	Unchecked	Globally enables IPSec on the router.
Aggressive mode	Checkbox	yes	Unchecked	Globally enables Aggressive mode on a router.
Name	String	Yes	Blank	Specifies a name for the tunnel.
Autostart Action	Dropdown Menu	Yes	Ignore	Specifies how the tunnel is initiated. Start On startup Route When traffic routes this way. Add Loads a connection without starting it. Ignore Ignores the connection.
Connection Type	Dropdown Menu	Yes	tunnel	Defines whether the connection is in tunnel or transport mode.
Remote GW address	IP address	Yes	None	Sets the public IP address of a remote peer.
Local Id	string	Yes	None	Defines the local peer identifier.
Remote Id	String	Yes	None	Sets the remote peer identifier.
Local LAN IP Address	String	Yes	None	Defines the local IP of LAN.
Local LAN IP Address Mask	String	Yes	None	Defines the local Mask of LAN.
Remote LAN IP Address	String	Yes	None	Defines the Remote IP of LAN.
Remote LAN IP Address Mask	String	Yes	None	Defines the Remote Mask of LAN.
Authby	Dropdown Menu	Yes	psk	Defines authentication method. Available options, psk, xauthpsk.
XAuth identity	String	No	None	Defines the identity/username the client uses to reply to an XAuth request. If not defined, the IKEv1 identity will be used as XAuth identity.
IKE algorithm	Dropdown Menu	Yes	aes128-sha1-modp2048, 3des-sha1-modp1536	Specifies the IKE algorithm to use. The format is: encAlgo-authAlgo-DHGroup encAlgo: 3des, aes, serpent, twofish, blowfish authAlgo: md5, sha, sha2 DHGroup: modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, modp8192
ESP algorithm	Dropdown Menu	Yes	aes128-sha1, 3des-sha1	Specifies the esp algorithm to use. The format is:

				encAlgo-authAlgo-PFSGroup encAlgo: 3des, aes, serpent, twofish, blowfish authAlgo: md5, sha, sha2 DHGroup: modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, modp8192 For example: aes128-sha1-modp1536. If no DH group is defined then PFS is disabled.
WAN interface	Dropdown Menu	Yes	None	Defines the WAN interface used by this tunnel.
IKE life time	Integer	Yes	3h	Specifies how long the keying channel of a connection (ISAKMP or IKE SA) should last before being renegotiated. Syntax: timespec: 1d, 2h, 25m, 10s.
Key life	Integer	Yes	1h	Specifies how long a particular instance of a connection, a set of encryption/authentication keys for user packets, should last, from successful negotiation to expiry. Normally, the connection is renegotiated, via the keying channel, before it expires (see rekeymargin). Syntax: timespec: 1d, 2h, 25m, 10s.
Rekey margin	Integer	Yes	9m	Margintime. Defines how long before a connection expiry or keying-channel expiry should begin to attempt to negotiate a replacement.
Keyring tries	String	Yes	3	Specifies how many attempts a positive integer or %forever should be made to negotiate a connection, or a replacement for one, before giving up. The value %forever means 'never give up'. It is only relevant locally; the other end does not need to agree on it.
DPD Action	Dropdown Menu	Yes	None	Valid values are none, clear, hold and restart. None Disables dead peer detection. Clear Clears down the tunnel if a peer does not respond. Reconnects

				when traffic brings the tunnel up. Hold Clears down the tunnel and bring up as soon as the peer is available. Restart Restarts DPD when no activity is detected.
DPD Delay	Integer	Yes	None	Defines the period time interval with which R_U_THERE messages/INFORMATIONAL exchanges are sent to the peer. These are only sent if no other traffic is received. Syntax: timespec: 1d, 2h, 25m, 10s.
DPD Timeout	Integer	Yes	150s	Defines the timeout interval, after which all connections to a peer are deleted in case of inactivity. Syntax: timespec: 1d, 2h, 25m, 10s.

Table 14: Connections fields for strongSwan IPSec VPN

From the Name field, type the **Connection Name**.

From the Autostart Action drop down menu, select **Ignore**.

From the Connection Type drop down menu, select **transport**.

From the Authby dropdown menu, select **psk**.

From the IKE algorithm dropdown menu, select the **encryption**, **hash algorithm** and **DH group**.

From the ESP algorithm dropdown menu, select the **encryption** and **hash algorithm**.

From the WAN Interface dropdown menu select the interface that is used to transmit IPSec packets.

In the IKE life time field, type the **Ike life time value**.

In the Key life field, type the **Key life value**.

In the Keying tries field, type a **%forever** value.

From the DPD Action drop down menu, select **clear**.

In the DPD Delay field, type a **DPD delay** value.

In the DPD Timeout field, type a relevant value.

At the bottom of the Secrets section, click **Add**.

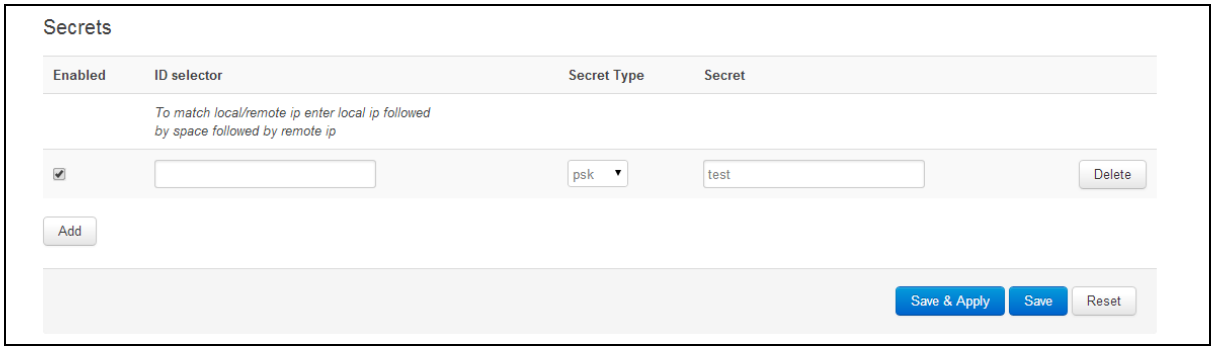


Figure 98: The secrets section

Select **Enabled**.

From the dropdown menu under Secret Type, select **psk**.

In the field beneath Secret, type the **psk password**.

Click **Save**.

29.4 DMVPN hub settings

In the top menu, select **Network -> DMVPN**. The DMVPN page appears.

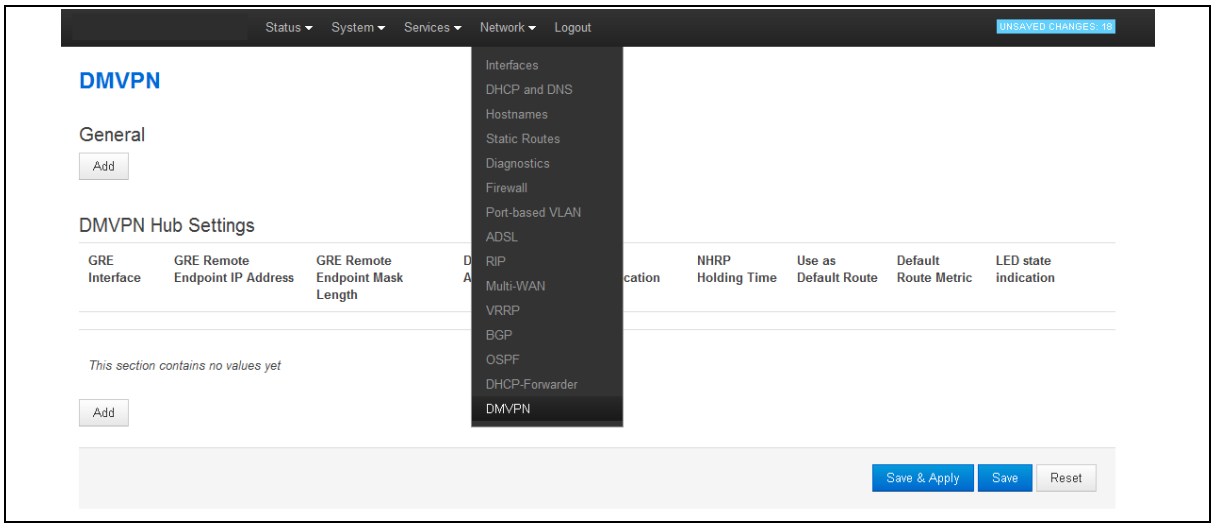


Figure 99: The DMVPN page

Under DMVPN General, click **Add**. The following page appears.

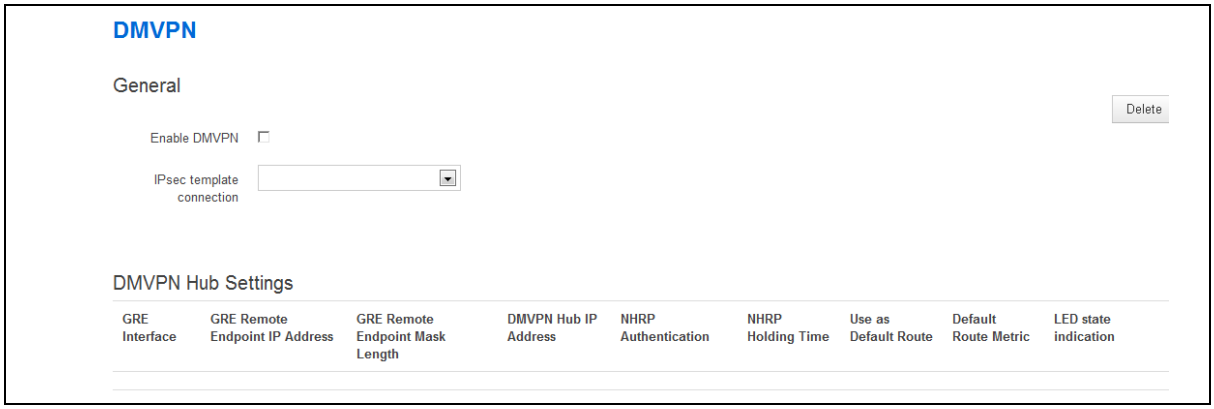


Figure 100: The DMVPN general section

Check **Enable DMVPN**.

From the IPSec template connection drop down menu, provide the **name of the IPsec connection**.

In the DMVPN Hub Settings section, click **Add**. The fields required to configure the parameters relative to the DMVPN Hub appear. These are used for the DMVPN tunnels, such as GRE tunnels, GRE tunnel remote IP, DMVPN Hub IP and password.

Name	Type	Required	Default	Description
GRE Interface	Dropdown list	Yes	Blank	Specifies which GRE interface will be used with this DMVPN configuration.
GRE Remote Endpoint IP Address	IP address	Yes	Blank	Configures the GRE IP address of the hub.
DMVPN Hub IP Address	IP address	Yes	Blank	Configures the physical IP address for the DMVPN hub.
NHRP Authentication	Numeric value	Yes	Blank	Enables authentication on NHRP. The password will be applied in plaintext to the outgoing NHRP packets. Maximum length is 8 characters.
NHRP Holding Time	Integer	Yes	Blank	Timeout for cached NHRP requests.

Table 15: DMVPN hub fields and their descriptions

29.5 UCI interface

29.5.1 IPSec configuration using CLI

You can configure IPSec (strongSwan package) through CLI using the UCI command suite.

Configuration files are stored at:

/etc/config/strongswan

To view the configuration file, use uci show strongswan or uci export strongswan commands.

```
root@GWxxxx:~# uci show strongswan
strongswan.general=general
strongswan.general.enabled=yes
strongswan.general.strictcrlpolicy=no
strongswan.general.uniqueids=yes
strongswan.general.cachecrls=yes
strongswan.general.nattraversal=yes
strongswan.@connection[0]=connection
strongswan.@connection[0].enabled=yes
strongswan.@connection[0].name=DMVPN
strongswan.@connection[0].type=transport
strongswan.@connection[0].localproto=gre
strongswan.@connection[0].remoteproto=gre
strongswan.@connection[0].ike=3des-md5-modp1024
strongswan.@connection[0].esp=aes128-sha1
strongswan.@connection[0].waniface=wan
strongswan.@connection[0].auto=ignore
strongswan.@connection[0].ikelifetime=28800s
strongswan.@connection[0].keylife=300s
strongswan.@connection[0].rekeymargin=30s
strongswan.@connection[0].keyingtries=%forever
strongswan.@connection[0].dpdaction=hold
strongswan.@connection[0].dpddelay=30s
strongswan.@connection[0].dpdtimeout=150s
strongswan.@secret[0]=secret
strongswan.@secret[0].enabled=yes
strongswan.@secret[0].secrettype=psk
strongswan.@secret[0].secret=secret
```

```
uci export strongswan

package strongswan

config general 'general'
        option enabled 'yes'
        option strictcrlpolicy 'no'
        option uniqueids 'yes'
        option cachecrls 'yes'
        option nattraversal 'yes'

config connection
        option enabled 'yes'
        option name 'DMVPN'
        option type 'transport'
        option localproto 'gre'
        option remoteproto 'gre'
        option ike '3des-md5-modp1024'
        option esp 'aes128-sha1'
        option waniface 'wan'
        option auto 'ignore'
        option ikelifetime '28800s'
        option keylife '300s'
        option rekeymargin '30s'
        option keyingtries '%forever'
        option dpdaction 'hold'
        option dpddelay '30s'
        option dpdtimeout '150s'

config secret
        option enabled 'yes'
        option secrettype 'psk'
        option secret 'secret'
```

29.6 Configuring DMVPN using CLI

You can configure DMVPN through CLI using the UCI command suite.

Configuration files are stored at:

/etc/config/dmvpn

To view the configuration file, use uci show dmvpn or uci export dmvpn commands.

```
uci export dmvpn

package dmvpn

config general-settings 'common'
        option enabled 'yes'
        option ipsec_template_name 'DMVPN'

config interface
        option holding_time '60'
        option gre_interface 'GRE'
        option gre_endpoint_ip '11.11.11.1'
        option gre_endpoint_mask_length '29'
        option nhs_ip '192.168.100.1'
        option cisco_auth 'test'

uci show dmvpn

dmvpn.common=general-settings
dmvpn.common.enabled=yes
dmvpn.common.ipsec_template_name=DMVPN
dmvpn.@interface[0]=interface
dmvpn.@interface[0].holding_time=60
dmvpn.@interface[0].gre_interface=GRE
dmvpn.@interface[0].gre_endpoint_ip=11.11.11.1
dmvpn.@interface[0].gre_endpoint_mask_length=29
dmvpn.@interface[0].nhs_ip=192.168.100.1
dmvpn.@interface[0].cisco_auth=test
```

To change any of the above values, use uci set command.

30 Terminal Server

30.1 Introduction

Terminal Server is a background application (a daemon) whose main task is to forward data between TCP connections or UDP streams and asynchronous serial ports.

Terminal Server application serves up to 4 sessions simultaneously one for each async serial port, depending on the device. Each Terminal Server session has an IP endpoint and an associated specific serial port.

30.2 Terminal Server interfaces

You can configure the IP endpoint of each Terminal Server session to be:

- TCP server: each session is listening on a unique port.
- TCP client: Terminal Server makes a TCP connection to external TCP server.
- UDP endpoint: Terminal Server forwards data between a UDP stream and a serial port.

30.3 Configuring Terminal Server

30.3.1 Configuring Terminal Server using the web interface

To access the Terminal Server configuration web interface, click **Services -> Terminal Server**. The Terminal Server Configuration page appears. You must configure two main sections: Main Settings and Port Settings.

30.3.1.1 Main settings

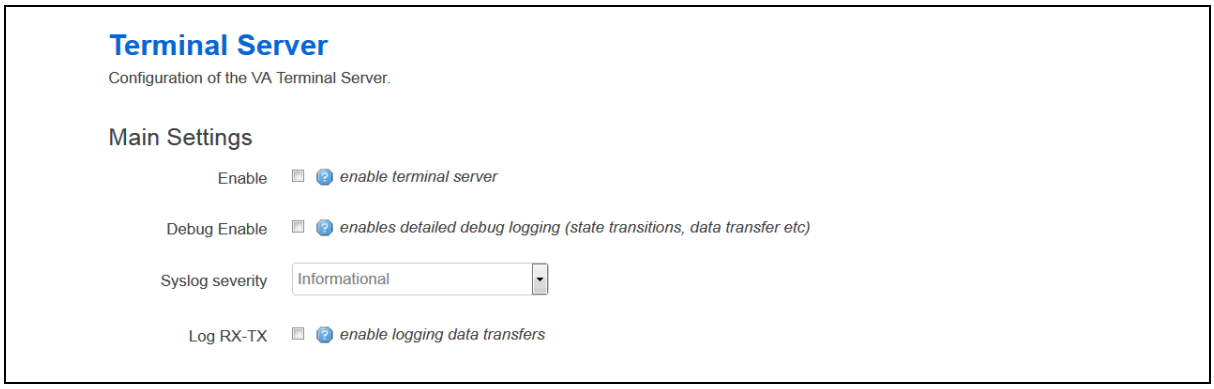


Figure 101: The terminal server main settings page

In the Main Settings section, click the **Enable** check box to enable the Terminal Server.

Name	Type	Required	Default	Description
Enable	Checkbox	Yes	Disabled	Enables the Terminal Server application.
Debug Enable	Checkbox	No	Disabled	Enables detailed debug logging.
Syslog severity	Dropdown list	Yes	Notice	Determines the syslog level. Events up to this priority will be logged. Emergency: 0 Alert: 1 Critical: 2 Error: 3 Warning: 4 Notice: 5 Info: 6 Debug: 7
Log Rx - Tx	Checkbox	No	Disabled	Enable logging data transfers.

Table 16: The main settings and their descriptions

30.3.1.2 Port settings

The Port Settings section is divided into 3 sub-sections:

- General
- Serial
- Network

30.3.1.3 Port settings: general section

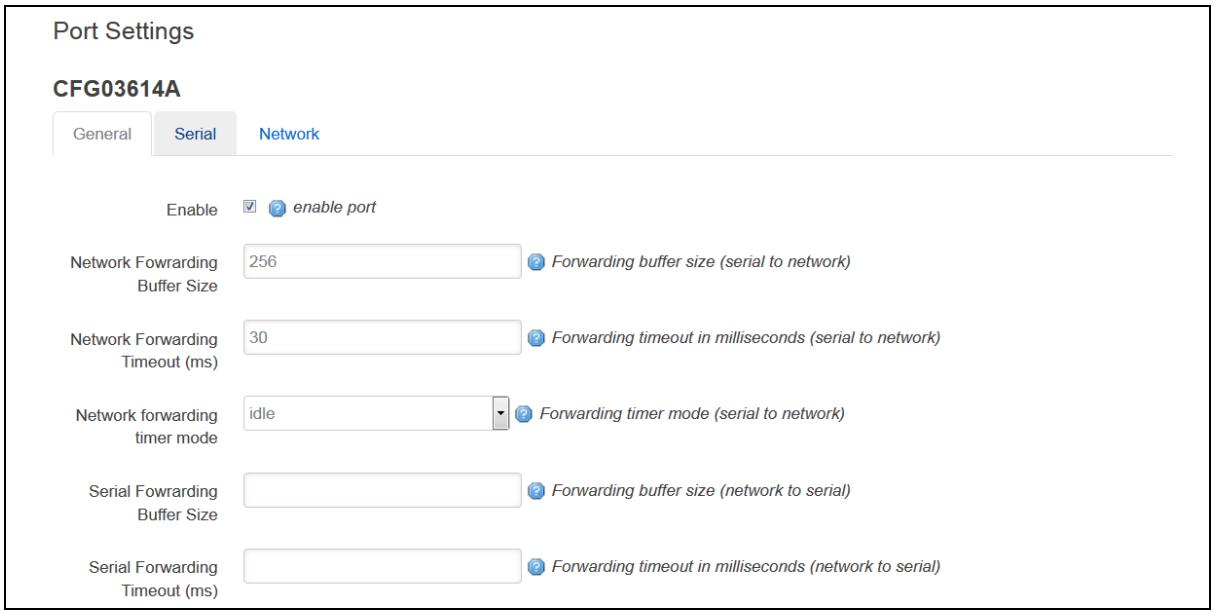


Figure 102: The General tab fields part 1

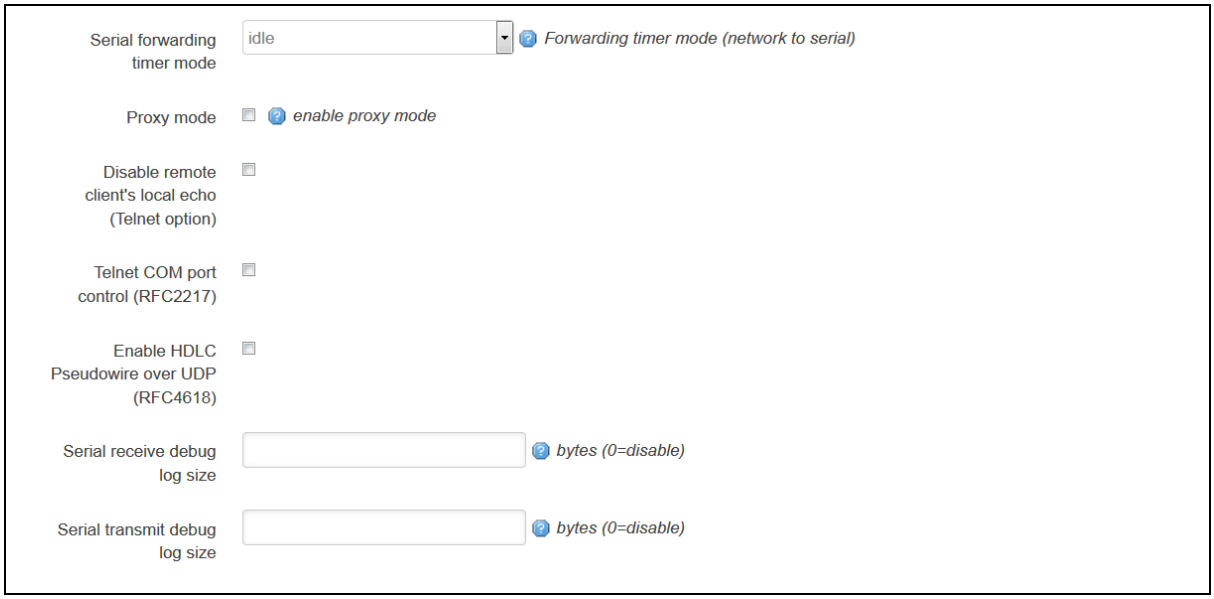

Serial forwarding timer mode
idle
Forwarding timer mode (network to serial)
Proxy mode
enable proxy mode
Disable remote client's local echo (Telnet option)
Telnet COM port control (RFC2217)
Enable HDLC Pseudowire over UDP (RFC4618)
Serial receive debug log size
bytes (0=disable)
Serial transmit debug log size
bytes (0=disable)

Figure 103: The general tab fields part 2

Name	Type	Required	Default	Description
Enable	Checkbox	Yes	Disabled	Enabled port.
Network Fowrarding Buffer Size	Numeric value	Yes	256	Forwarding buffer size (serial to network).
Network Forwarding Timeout	Numeric value	Yes	30	Forwarding timeout in milliseconds (serial to network).
Network forwarding timer mode	Dropdown list	Yes	idle	Forwarding timer mode (serial to network), 'idle'=timer re-started on each received data, 'aging'=timer started on first rx.
Serial Fowrarding Buffer Size	Numeric value	No	0	Forwarding buffer size (network to serial), 0=use maximum possible network rx buffer size.
Serial Forwarding Timeout (ms)	Numeric value	No	20	Forwarding timeout in milliseconds (network to serial), 0=forward to serial immediately.
Serial forwarding timer mode	Dropdown list	Yes	idle	Forwarding timer mode (network to serial), 'idle'=timer re-started on each received data, 'aging'=timer started on first rx.
Proxy mode	Checkbox	No	Disabled	Enable proxy mode.
Disable remote client's local echo (Telnet option)	Checkbox	No	Disbled	1=send IAC WILL ECHO Telnet option to remote client forcing it to disable local echo (for server mode only).
Telnet COM port control (RFC2217)	Checkbox	No	Disbled	1=enable support for Telnet COM port control (RFC2217).
Enable HDLC Pseudowire over UDP (RFC4618)	Checkbox	No	Disabled	Enables HDLC Pseudowire over UDP support (based on RFC4618), if set to 1, also set udpMode 1.

Serial receive debug log size	Numeric value	No	Disabled	Configures serial receive log size in bytes and enables receive data logging. 0=disabled.
Serial transmit debug log size	Numeric value	No	Disabled	Configures serial transmit log size in bytes and enables transmit data logging. 0=disabled.

Table 17: The general fields descriptions

30.3.1.4 Port settings: serial section

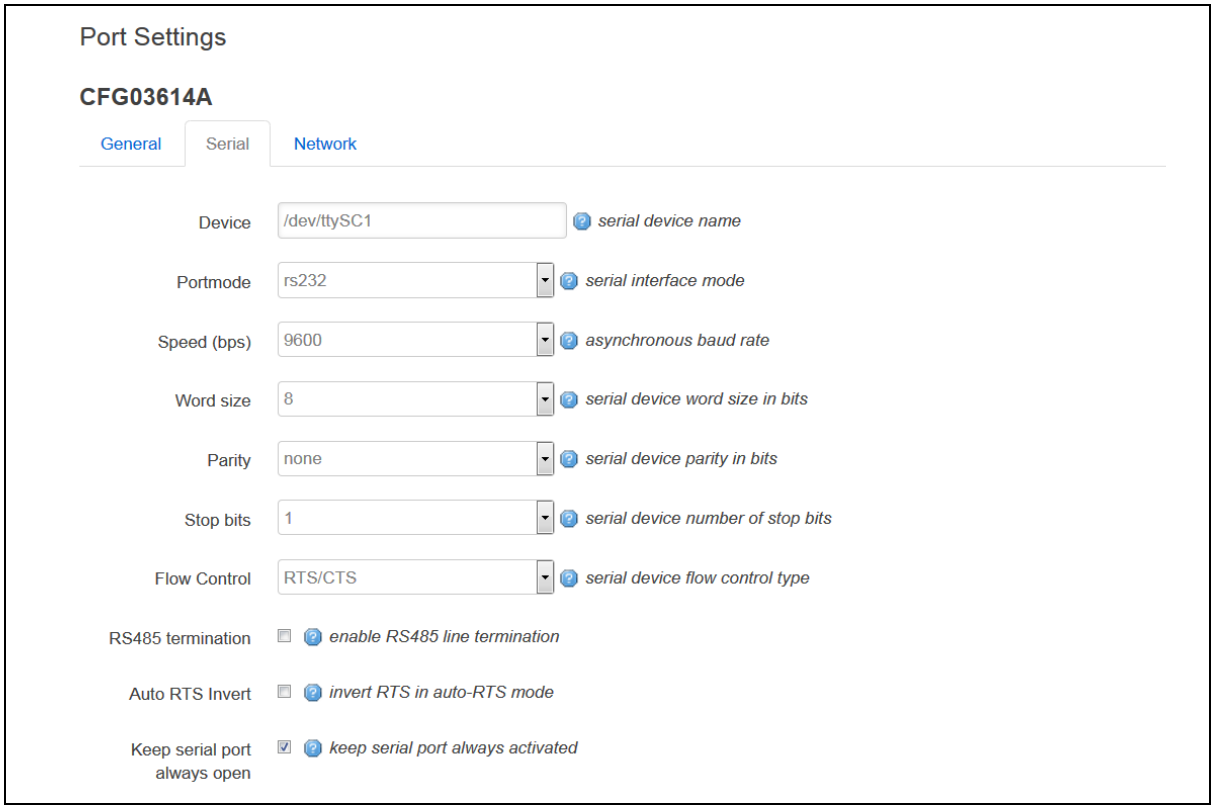


Figure 104: The serial tab fields part 1

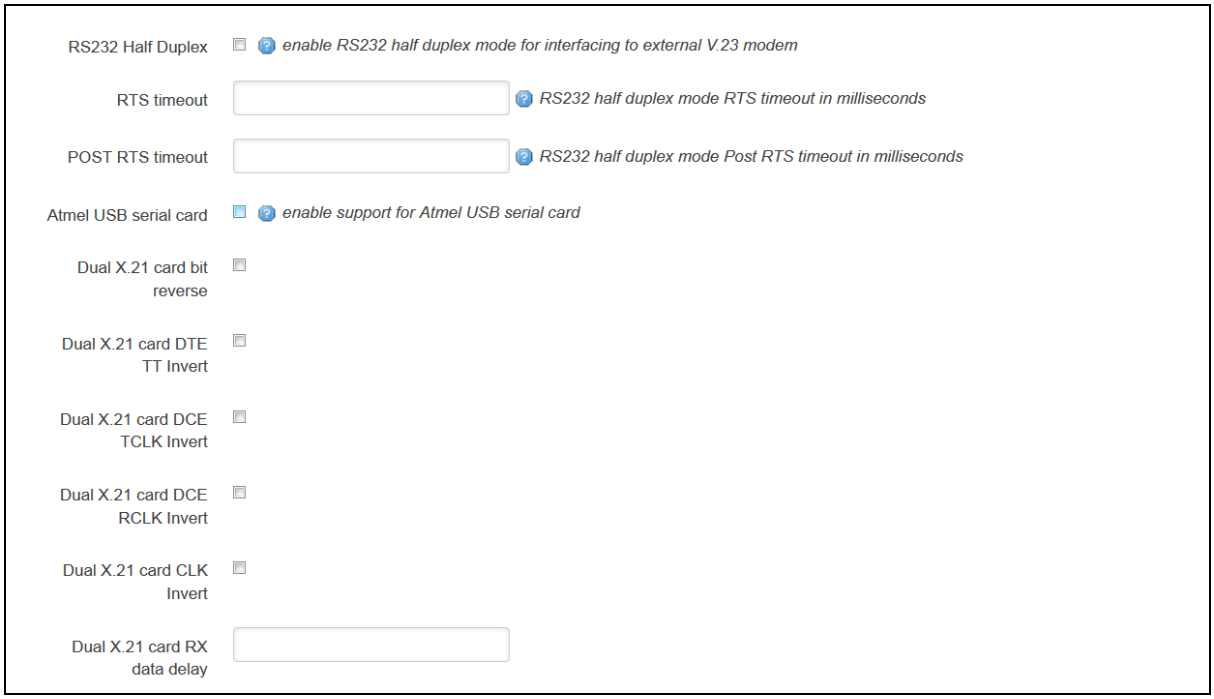

RS232 Half Duplex
enable RS232 half duplex mode for interfacing to external V.23 modem
RTS timeout
RS232 half duplex mode RTS timeout in milliseconds
POST RTS timeout
RS232 half duplex mode Post RTS timeout in milliseconds
Atmel USB serial card
enable support for Atmel USB serial card
Dual X.21 card bit reverse
Dual X.21 card DTE TT Invert
Dual X.21 card DCE TCLK Invert
Dual X.21 card DCE RCLK Invert
Dual X.21 card CLK Invert
Dual X.21 card RX data delay

Figure 105: The serial tab fields part 2

Name	Type	Required	Default	Description
Device	String	Yes	'/dev/ttySC0' '/dev/ttySC1'	Serial device name.
Portmode	Dropdown list	Yes	rs232	rs232 - RS-232 mode, rs485hdx - rs485 2 wire half duplex mode in which transmitter drives RTS. rs485fdx - RS485 4 wire full duplex mode. 'v23' - using V.23 leased line card driver. x21 - use USB serial card in sync mode.
Speed (bps)	Dropdown list	Yes	9600	Serial device speed in baud.
Word size	Dropdown list	Yes	8	Serial device word size (5,6,7,8).
Parity	Dropdown list	No	0	Serial device parity (0=none, 1=even, 2=odd).
Stop bits	Dropdown list	Yes	1	Serial device number of stop bits (1 or 2).
Flow Control	Dropdown list	No	0	Serial flow control mode (0=none, 1=RTS CTS, 2=XONXOFF).
RS485 termination	Checkbox	No	0	Enables or disables RS485 line termination (applies only if portmode is 'rs485').
Auto RTS Invert	Checkbox	No	0	Invert RTS in auto-RTS mode (if portmode is 'rs485').
Keep serial port always open	Checkbox	No	0	Keep serial port always open (if option not present, default is 0).
RS232 Half Duplex	Checkbox	No	0	1=half duplex mode; 0=full duplex

				mode.
RTS timeout	Numeric value	No	30	In RS232 half duplex mode, time in milliseconds between raising RTS and enabling the transmitter.
POST RTS timeout	Numeric value	No	20	In RS232 half duplex mode, time in milliseconds between dropping RTS (transmission finished) and enabling the receiver.
Atmel USB serial card	Checkbox	No	0	This configures the use of tservd with the Atmel USB serial card.
Dual X.21 card bit reverse	Checkbox	No	0	Enables bit reversal of all bits in 8 byte word during transmission.
Dual X.21 card DTE TT Invert	Checkbox	No	0	Enables X.21 TT clock signal inversion.
Dual X.21 card DCE TCLK Invert	Checkbox	No	0	Enables X.21 DCE TCLK signal inversion.
Dual X.21 card DCE RCLK Invert	Checkbox	No	0	Enables X.21 DCE RCLK signal inversion.
Dual X.21 card CLK Invert	Checkbox	No	0	Enables X.21 DCE CLK signal inversion.
Dual X.21 card RX data delay	Numeric value	No	0	Sets X.21 card RX data delay in number of bit positions.

Table 22: The general fields descriptions

30.3.1.5 Port settings: network section

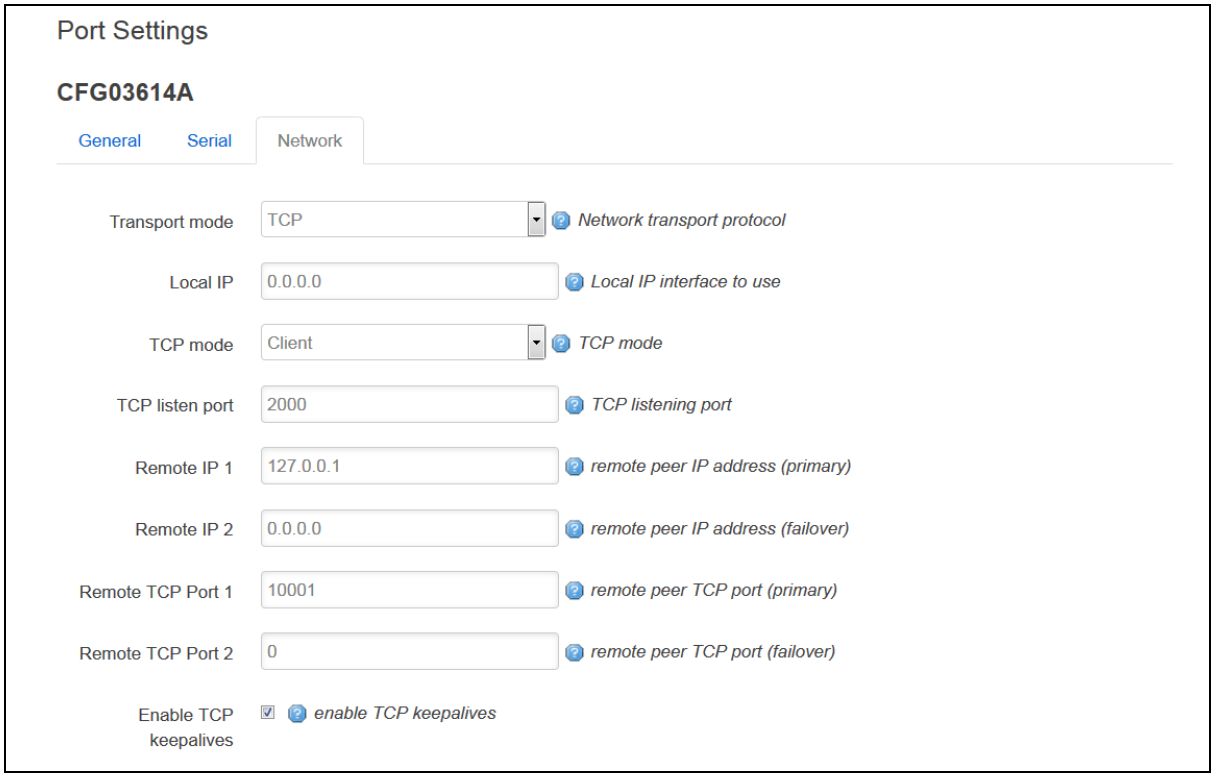


Figure 106: The Network tab fields part 1

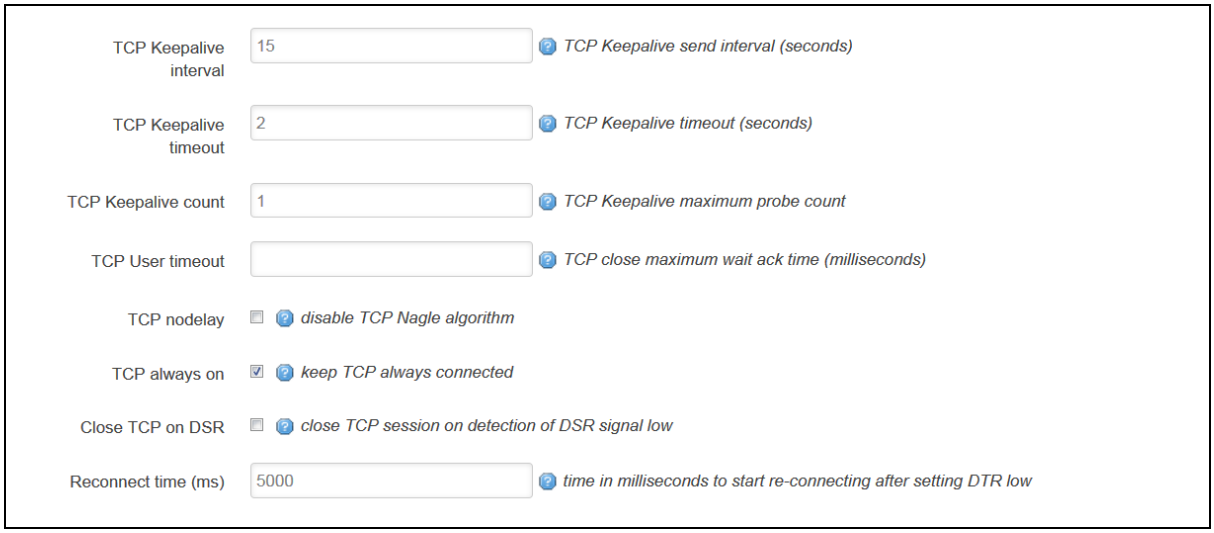


Figure 1071: The Network tab fields part 2

Name	Type	Required	Default	Description
Transport mode	Dropdown list	Yes	TCP	Select between TCP/UDP.
Local IP	IP address	Yes	0.0.0.0	Local IP address to listen on (0.0.0.0=listen on any interface).
TCP mode	Dropdown list	Yes	Server	Select between server and client modes of TCP.
TCP listen port	Numeric value	Yes	999	TCP listen port for server mode.
Remote IP 1	IP address	Yes	0.0.0.0	Destination peer IP 1address
Remote IP 2	IP address	Yes	0.0.0.0	Destination peer IP 2 address(for failover).
Remote TCP Port 1	Numeric value	Yes	951	Destination peer port IP 1 number.
Remote TCP Port 2	Numeric value	Yes	951	Destination peer port IP 2 number(for failover).
Enable TCP keepalives	Checkbox	No	Enabled	Enable or disable TCP keep alives.
TCP Keepalive interval	Numeric value	No	5	Interval in seconds between TCP keep alive probes.
TCP Keepalive timeout	Numeric value	No	2	Time in seconds to wait for reponse to a TCP keep alive probe.
TCP Keepalive count	Numeric value	No	1	Number of TCP keep alive probes to send before connection closed.
TCP User timeout	Numeric value	No	0	Maximum time in milliseconds for TCP to wait for transmitted data to be acked before closing connection in established state. Set to 0 to use kernel defaults (about 15-20 minutes).
TCP nodelay	Checkbox	No	Disabled	1=disable TCP nagle algorithm;

				0=normal operation.
TCP always on	Checkbox	No	Disabled	Keep TCP session always connected.
Close TCP on DSR	Checkbox	No	Disabled	Close TCP session on detection of DSR signal low.
Reconnect time (ms)	Numeric value	No	5000	Time in milliseconds to start re-connecting after setting DTR low.

Table 18: The Network fields descriptions

30.4 Configuring Terminal Server using UCI

You can also configure Terminal Server through CLI using UCI command suite.

The configuration file is stored at:

/etc/config/tservd

To view the configuration file, use commands:

uci export

or

uci show

The global configuration section contains two parameters. The meaning of the parameters is explained in the embedded comments:

```
config tservd main
    # set to 1 to enable Terminal Server
    option enable 1
# enables detailed debug logging (state transitions, data transfer etc)
    option debug_ev_enable 1
```

Following the global section there are four port specific sections. Below is an example configuration with the embedded comments explaining each parameter.

```
config tservd main
    # set to 1 to enable terminal server
    option enable 0

    # enables detailed debug logging (state transisions, data transfer etc)
    option debug_ev_enable 0

    # sets syslog level (0 to 7), default is 6
    option log_severity 6

config port 'port1'
    # enables this port
    option enable 0

    # serial device name
    option devName '/dev/ttySC0'

    # destination peer port IP number (two number for failover)
    option ip_port1 951
    option ip_port2 951

    # destination peer ip address (two addresses for failover)
    option remote_ip1 '0.0.0.0'
    option remote_ip2 '0.0.0.0'

    # keep TCP session always connected
    option tcp_always_on 1

    # close TCP session on detection of DSR signal low
    option close_tcp_on_dsr 0

    # keep serial port always open (if option not present, default is 0)
    option tty_always_open 0

    # Forwarding timeout in milliseconds (serial to network)
    option fwd_timeout 30
```

```
    # Forwarding timer mode (serial to network), 'idle'=timer re-started on
each received data, 'aging'=timer started on first rx
    option fwd_timer_mode 'idle'

    # Forwarding buffer size (serial to network)
    option fwd_buffer_size 256

    # Forwarding buffer size (network to serial), 0=use maximum possible
network rx buffer size
    option sfwd_buffer_size 0

    # Forwarding timeout in milliseconds (network to serial), 0=forward to
serial immediately
    option sfwd_timeout 20

    # Forwarding timer mode (network to serial), 'idle'=timer re-started on
each received data, 'aging'=timer started on first rx
    option sfwd_timer_mode 'idle'

    # serial device speed in baud
    option speed 115200

    # serial device word size (5,6,7,8)
    option wsize 8

    # serial device parity (0=none, 1=even, 2=odd)
    option parity 0

    # serial device number of stop bits (1 or 2)
    option stops 1

    # serial flow control mode (0=none, 1=RTS CTS, 2=XONXOFF)
    option fc_mode 0

    # time in milliseconds to start re-connecting after setting DTR low
    option disc_time_ms 5000
```

```
    # TCP server mode
    option server_mode 1

    # Proxy mode (off by default)
    option proxy_mode 0

    # Local IP address to listen on (0.0.0.0=listen on any interface)
    option local_ip '0.0.0.0'

    # TCP listen port for server mode
    option listen_port 999

    # UDP mode
    option udpMode 0

    # UDP local port UDP mode
    option udpLocalPort 0

    # UDP port for UDP mode
    option udpRemotePort 0

    # If set to non zero, send empty UDP packets every this many
milliseconds to remote peer
    option udpKaIntervalMs 0

    # Max number of consecutive remote UDP keepalive missed (not received)
before UDP session considered broken
    option udpKaCount 3

    # Enable or disable TCP keep alives
    option tcp_keepalive_enabled 1

    # Interval in seconds between TCP keep alive probes
    option tcp_keepalive_interval 5

    # Time in seconds to wait for reponse to a TCP keep alive probe
    option tcp_keepalive_timeout 2
```

```
    # Number of TCP keep alive probes to send before connection closed
    option tcp_keepalive_count 1

    # Maximum time in milliseconds for TCP to wait for transmitted data to
be acked
    # before closing connection in established state. Set to 0 to use
kernel defaults (about 15-20 minutes)
    option tcp_user_timeout 20000

    # 1=disable TCP nagle algorithm; 0=normal operation
    option tcp_nodelay 0

    # rs232 - RS-232 mode, rs485hdx - rs485 2 wire half duplex mode in
which transmitter drives RTS. rs485fdx - RS485 4 wire full duplex mode.
'v23' - using V.23 leased line card driver. x21 - use USB serial card in
sync mode
    option portmode 'rs232'

    # On newer GW202x boards, the serial mode (RS232, RS485) for the second
physical port is set with GPIOs, while on older boards it is set with the
dip switches
    # 1=On this port, the serial mode is set using GPIO; 0=Default, serial
mode is set with dip switches
    option serial_mode_gpio_control 0

    # Driver DTR and RTS line control modes. 'auto' - set ON when the port
is open, OFF when the port is closed, 'on' - always on, 'off' - always off,
'app' - controlled by the application, 'ontx' - in HDLC mode, RTS ON during
frame TX
    option dtr_control_mode 'auto'
    option rts_control_mode 'auto'

    # enables or disables RS485 line termination (applies only if portmode
is 'rs485')
    option rs485_line_termination '0'

    # 1=use USB serial card. if portmode is x.21 it is used in synchronous
mode, if portmode is 'rs232' it is used in asynchronous mode
```

```
    option is_usb_serial 0

    # Used for USB serial card. 'hdlc' = synchronous HDLC framed mode;
'transp' = transparent mode
    option sync_mode 'hdlc'

    # Used for USB serial card. 1= in HDLC mode use CRC32; 0= use CRC16
    option sync_crc32 0

    # Used for USB serial card. Synchronous speed, If not 0, use internal
clock, example speeds: 9600, 19200, 64000, 128000, 256000, 384000, 512000,
768000, 1024000, 2048000, 0=use external clock
    option sync_speed '64000'

    # Used for USB serial card. Enables receive clock inversion. 0=data
sampled on clock falling edge; 1=data sampled on clock rising edge
    option sync_invert_rxclk 0

    # Used for USB serial card. Enables transmit clock inversion. 0=data
out on clock falling edge; 1=data out on clock rising edge
    option sync_invert_txclk 0

    # Used for USB serial card. 1=receive most significant bit first;
0=receive least significant bit first
    option sync_rx_msbf 0

    # Used for USB serial card. 1=transmit most significant bit first;
0=transmit least significant bit first
    option sync_tx_msbf 0

    # Used for USB serial card. Number of bit positions to delay sampling
the data from detecting clock edge
    option sync_rxdata_dly 0

    # Used for USB serial card. Number of bit positions to delay output of
the data from detecting clock edge
    option sync_txdata_dly 0
```

```
    # Used for USB serial card. Value of idle character (decimal) to
transmit in case of TX underrun (0 to 255)
    # in HDLC mode configures inter-frame fill: set to 0 to transmit 0s,
255 to transmit 1s, 126 to transmit flags
    option sync_tx_idle 126

    # Invert RTS in auto-RTS mode (if portmode is 'rs485')
    option rtsinvert '0'

    # 1=send IAC WILL ECHO Telnet option to remote client forcing it to
disable local echo (for server mode only)
    option disable_echo 0

    # 1=enable support for Telnet COM port control (RFC2217)
    option com_port_control 0

    # 1=half duplex mode; 0=full duplex mode
    option hd_mode 0

    # in RS232 half duplex mode, time in milliseconds between raising RTS
and enabling the transmitter
    option rts_timeout 30

    # in RS232 half duplex mode, time in milliseconds between dropping RTS
(transmission finished) and enabling the receiver
    option post_rts_timeout 20

    # when used with V.23 modem driver, (set portmode 'v23'), transmit
samples are multiplied by this value
    option v23_tx_gain '2'

    # when used with V.23 modem driver, (set portmode 'v23'), received
samples are divided by this value
    option v23_rx_loss '1'

    # when used with V.23 modem driver, (set portmode 'v23') V.23 modem's
RTS to CTS delay in milliseconds
    option v23_rts_to_cts_delay '20'
```

```
    # when used with V.23 modem driver, (set portmode 'v23') LIM operation:
0=2wire; 1=4wire
    option v23_is_four_wire '0'

    # when used with V.23 modem driver, (set portmode 'v23'), sets the
receive echo suppression timeout in milliseconds
    option v23_tx_timeout '20'

    # when used with V.23 modem driver, (set portmode 'v23'), time in
milliseconds it takes V.23 transmitter to rampdown carrier from peak to
zero
    option v23_tx_rampdown '30'

    # when used with V.23 modem driver, (set portmode 'v23'), sets the
maximum transmit fifo fill level in bytes
    option v23_tx_maxfill '127'

    # when used with V.23 modem driver, (set portmode 'v23'), enables
signalling of carrier by sending special characters
    option v23_inband_carrier_signalling '0'

    # when used with V.23 modem driver, (set portmode 'v23'), this
character decimal value signalls remote carrier on
    option v23_inband_carrier_on_char '255'

    # enables HDLC Pseudowire over UDP support (based on RFC4618), if set
to 1, also set udpMode 1
    option hdlc_pw_enabled 0

    # Configures serial transmit log size in bytes and enables transmit
data logging. 0=disabled
    option serialTxLogSize 0

    # Configures serial receive log size in bytes and enables receive data
logging. 0=disabled
    option serialRxLogSize 0
```

```
# bit reverse: 0=normal; 1=reverse
option bit_reverse 0

# v24 dte tt clock invert: 0=normal; 1=invert
option dte_tt_inv 0

# v24 dce tx clock invert: 0=normal; 1=invert
option dce_tclk_inv 0

# v24 dce rx clock invert: 0=normal; 1=invert
option dce_rclk_inv 0

# x21 clock invert: 0=normal; 1=invert
option x21_clk_invert 0

# x21 data delay: 0-7 - delay in local clk or VCO clock cycles
option x21_data_delay 0

# destination peer ip address (two addresses for failover)
option remote_ip1 '10.1.10.211'
option remote_ip2 '0.0.0.0'

# keep TCP session always connected
option tcp_always_on 0

# close TCP session on detection of DSR signal low
option close_tcp_on_dsr 1
# Forwarding timeout in milliseconds (serial to network)
option fwd_timeout 30

# Forwarding buffer size (serial to network)
option fwd_buffer_size 256

# Receive control characters that cause buffer to be forwarded
option rcc_string ''

# serial device speed in baud
```

```
    option speed 115200

    # serial device word size (5,6,7,8)
    option wsize 8

    # serial device parity (0=none, 1=even, 2=odd)
    option parity 0

    # serial device number of stop bits (1 or 2)
    option stops 1

    # serial from control mode (0=none, 1=RTS CTS, 2=XONXOFF)
    option fc_mode 1

    # time in milliseconds to start re-connecting after setting DTR low
    option disc_time_ms 5000

    # TCP server mode
    option server_mode 1

    # TCP listen port for server mode
    option listen_port 999

    # UDP mode
    option udpMode 0

    # UDP port for UDP mode
    option udpPort 0
```

Each Terminal Server port must be associated with a specific serial port device. For example, you can configure port 1 as:

```
config tservd port1
    # enables this port
    option enable 1

    # serial device name
    option devName '/dev/ttySC1'

    ….. other options follow ….
```

30.5 Terminal Server operation

30.5.1 General

The Terminal Server package consists of two binaries:

- tservd – Terminal Server deamon, full path at /usr/sbin/tservd
- tserv – Terminal Server command line interface, path at /usr/sbin/tserv

30.5.2 Starting Terminal Server

By default, if Terminal Server is enabled in /etc/config/tservd, it is started on boot up automatically. To start Terminal Server manually, enter:

/usr/sbin/tservd

30.5.3 Checking the status of Terminal Server

To check if Terminal Server is running, enter:

ps | grep tservd.

If Terminal Server is running there it will be shown with its process ID, in the following example, the process ID (PID) is 1264:

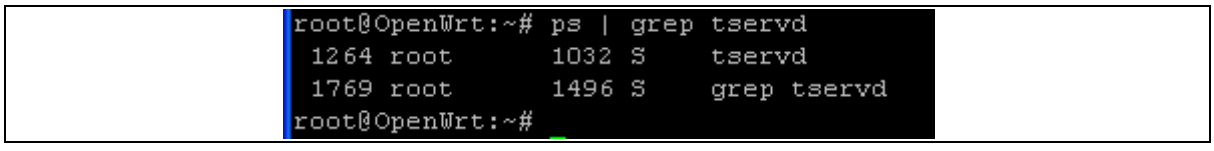


Figure 108: Output from the command line ps | grep tservd

Alternatively, run: **/usr/bin/tserv show stats**

If the Terminal Server is running, this command will show the status of each session. If the Terminal Server is not loaded it will return an error.

30.5.4 Stopping Terminal Server

Sometimes it may be necessary to stop Terminal Server, for example if the configuration is changed and it is not desirable to reboot the router.

To stop Terminal Server, enter one of the following:

/usr/bin/tserv quit

Kill PID. You can obtain the PID by running: **ps | grep tser**

31 GRE interfaces

General Routing Encapsulation (GRE) is a tunnelling protocol used for encapsulation of other communication protocols inside point to point links over IP.

31.1 GRE web interface

To create GRE interfaces through the web interface, in the top menu, select **Network ->Interfaces -> Add new interface**.

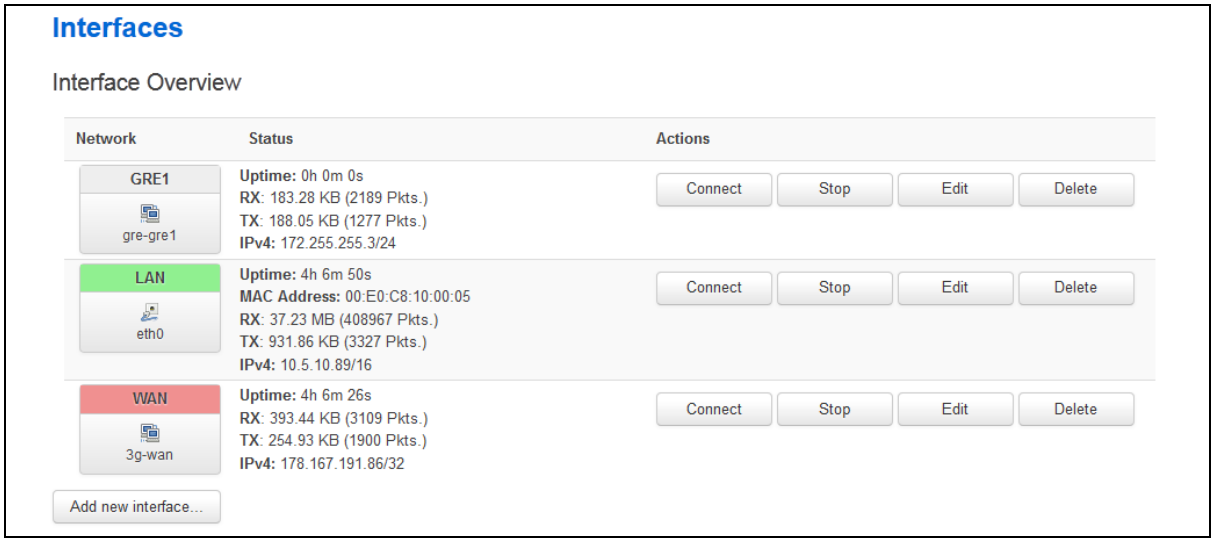


Figure 109: The interfaces page

Click **Add new interface**.

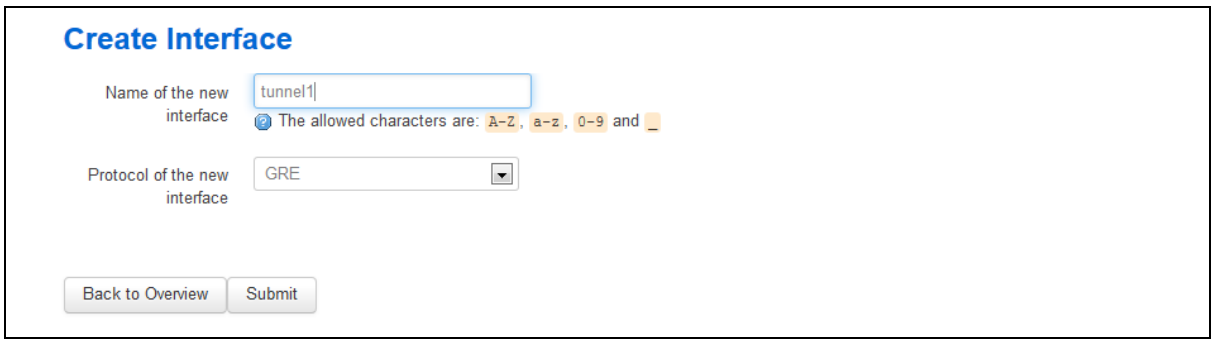


Figure 110: The create interface page

Type in the name of the new interface, then in the Protocol of the new interface drop-down list, select **GRE**.

Name	Type	Required	Default	Description
Name of the new interface	Text	yes	Blank	Assigns a logical name to the GRE tunnel.
Protocol of the new interface	Dropdown list	yes	Static	Specifies what protocol the interface will operate on. For example, GRE.

Table 19: The create interface field descriptions

When you have made your configuration changes, click **Submit**. The GRE interface details page appears. Use this page to configure tunnel source IP and mask, the interface the tunnel will be attached to, TLL, tunnel key ID, and MTU.

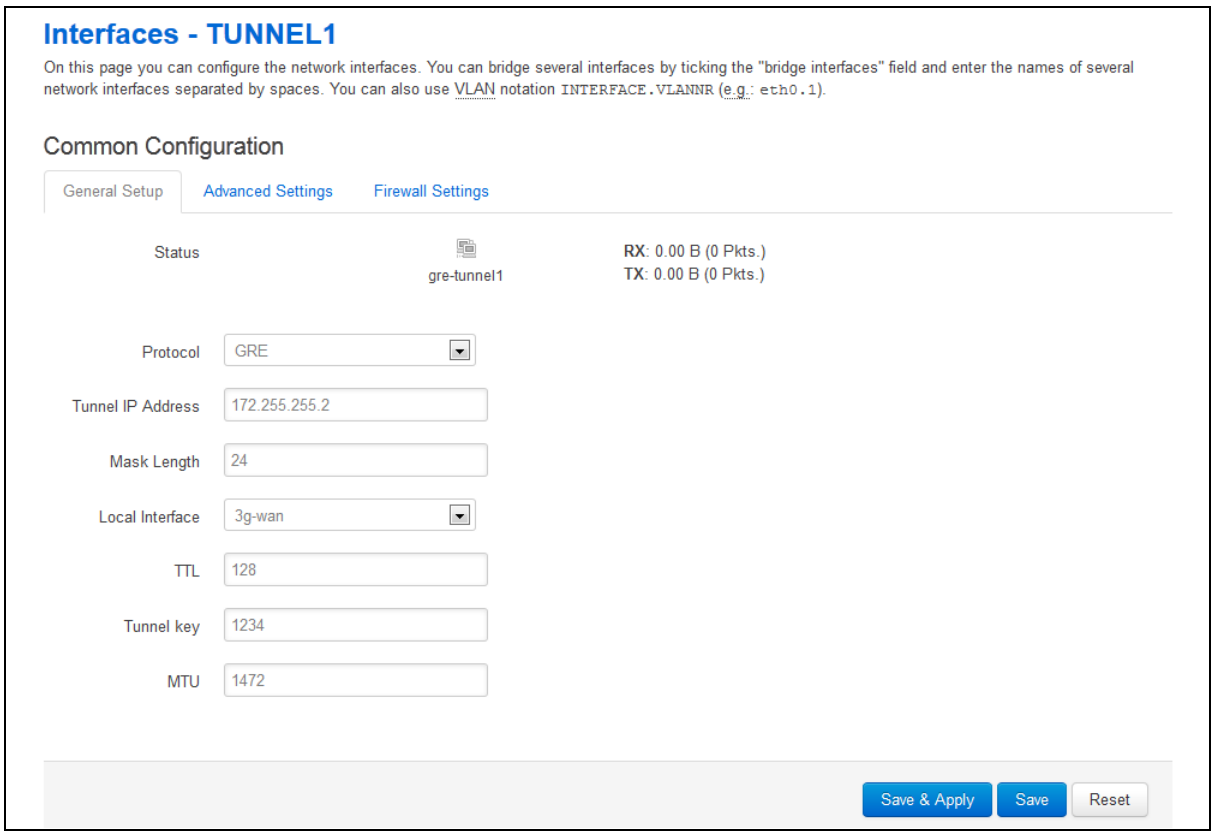


Figure 111: The interfaces – tunnel page

When you have made your configuration changes, click **Save and Apply**.

Name	Type	Required	Default	Description
Protocol	Dropdown list	Yes	Blank	Configures a logical name to the GRE tunnel.
Tunnel IP Address	IP address	Yes	Blank	Configures local IP address of the GRE interface.
Mask Length	Dropdown list	Yes	Static	Specifies what protocol the interface will support. For example, GRE.
Local Interface	Dropdown list	Yes	Blank	Specifies which interface is going to be linked with the GRE tunnel interface.
TTL	Numeric	Yes	128	Sets Time-To-Live value on the

	value			interface.
Tunnel key	Numeric value	Yes	Blank	Sets GRE tunnel key.
MTU	Numeric value	Yes	1472	Configures MTU (maximum transmission unit) size of PDUs using this interface.

Table 20: Interfaces –Tunnel page fields and their descriptions

31.2 GRE UCI interface

You can also configure GRE UCI through CLI using UCI command suite.

The configuration file is stored at:

/etc/config/network

To view the configuration file, use the commands:

uci export network

or

uci show network

```
~# uci export network
config interface 'tunnel1'
        option proto 'gre'
        option ipaddr '172.255.255.2'
        option mask_length '24'
        option local_interface '3g-wan'
        option ttl '128'
        option key '1234'
        option mtu '1472'

~# uci show network
network.tunnel1=interface
network.tunnel1.proto=gre
network.tunnel1.ipaddr=172.255.255.2
network.tunnel1.mask_length=24
network.tunnel1.local_interface=3g-wan
network.tunnel1.ttl=128
network.tunnel1.key=1234
network.tunnel1.mtu=1472
```

© Virtual Access 2015

Name	Type	Required	Default	Description
proto	Interface	Yes	Blank	Configures a logical name to the GRE tunnel.
ipaddr	IP address	Yes	Blank	Configures local IP address of the GRE interface.
mask_length	IP address	Yes	Blank	Specifies what protocol the interface will support. For example, GRE.
local_inerface	Interface	Yes	Blank	Specifies which interface is going to be linked with the GRE tunnel interface.
ttl	Numeric value	Yes	128	Sets Time-To-Live value on the interface.
key	Numeric value	Yes	Blank	Sets GRE tunnel key.
mtu	Numeric value	Yes	1472	Configures MTU (maximum transmission unit) size of PDUs using this interface.

Table 21: Config interface fields and their descriptions

To change any of the above values use `uci set` command.

32 Multicasting using PIM and IGMP interfaces

IP multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to potentially thousands of corporate recipients. Applications that take advantage of multicast include video conferencing and corporate communications.

IP multicast delivers application source traffic to multiple receivers without burdening the source or the receivers while using a minimum of network bandwidth.

PIM (Protocol Independent Multicast) and IGMP (Internet Group Management Protocol) are protocols used to create multicasting networks within a regular IP network.

A multicast group is an arbitrary group of receivers that expresses an interest in receiving a particular data stream. The receivers (the designated multicast group) are interested in receiving a data stream from the source. They indicate this by sending an Internet Group Management Protocol (IGMP) host report to their closest router in the network. The routers are then responsible for delivering the data from the source to the receivers. The routers use Protocol Independent Multicast (PIM) between themselves to dynamically create a multicast distribution tree. The data stream will then be delivered only to the network segments that are in the path between the source and the receivers.

To summarize: PIM is used between routers while IGMP is used between a receiver and its router only. As a result, PIM must be enabled on all the interfaces on the route from the multicast source to the multicast client while IGMP must be enabled on the interface to the multicast client only.

32.1 Configuring PIM and IGMP via the web interface

To configure PIM through the web interface, in the top menu, select Network -> PIM. The PIM page appears.

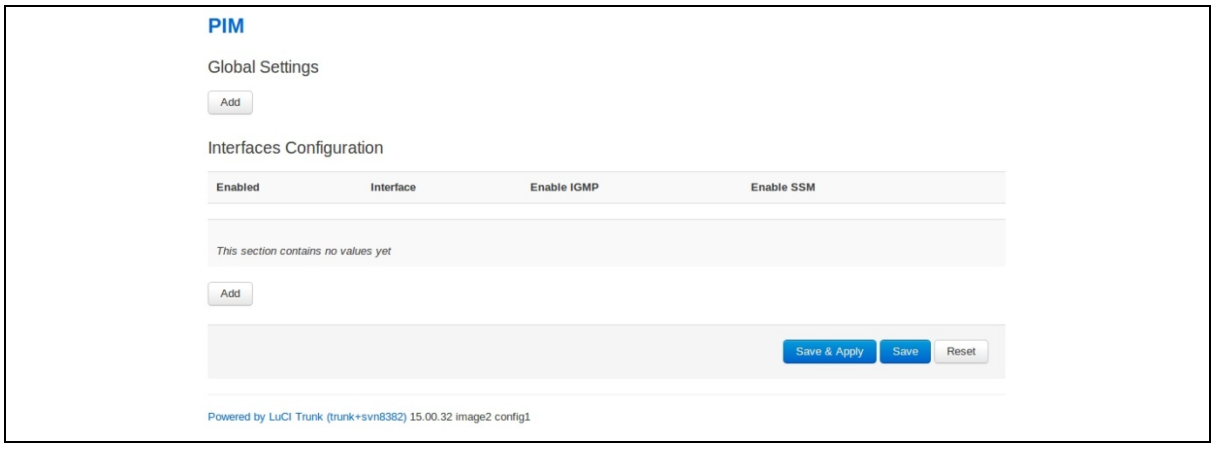


Figure 112: The PIM page

In the PIM page, click **Add**. The Global Settings section appears.

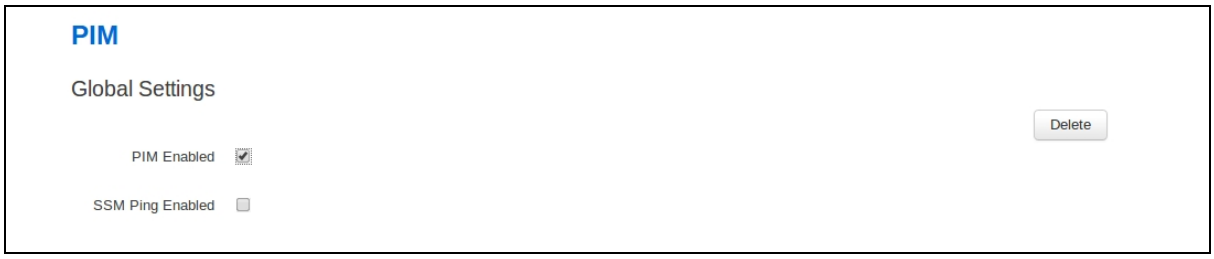


Figure 113: The global settings interface

Enable PIM by checking **PIM Enabled**.

Name	Type	Required	Default	Description
PIM Enabled	Checkbox	yes	Unchecked	Globally enable PIM on the router
SSM Ping Enabled	Checkbox	yes	Unchecked	Enable answers to SSM pings

Table 22: The PIM global settings description

Scroll down to the Interfaces Configuration section and click **Add**.

Figure 114: The interfaces configuration section

In the interface drop down list, choose the interface you wish to enable PIM on.

Check **Enabled** to allow the interface to be managed by the PIM application.

Check either **Enable SSM** and/or **Enable IGMP** depending on your requirements.

Note: you must enable PIM SSM on all the interfaces on the route from the multicast source to the multicast client

IGMP must be enabled on the interface to the multicast client only.

Name	Type	Required	Default	Description
Enabled	Checkbox	yes	Unchecked	Enable management of the given interface by the PIM application.
Interface	Drop down list	yes	Blank	Select the interface to apply the settings to.
Enable IGMP	Checkbox	yes	Unchecked	Enable IGMP on given interface.
Enable SSM	Checkbox	yes	Unchecked	Enable SSM on given interface.

Table 23: The PIM global settings description

To save your configuration updates, click **Save & Apply**.

32.2 PIM and IGMP UCI interface

You can configure PIM and IGMP through CLI using UCI.

The configuration file is stored at:

/etc/config/pimd

To view the configuration file, use commands:

uci export pimd

or

uci show pimd

```
root@VA_router:/etc/config1# uci export pimd
package pimd
config routing 'pimd'
        option enabled 'yes'

config interface
        option enabled 'yes'
        option interface 'lan'
        option ssm 'yes'
        option igmp 'yes'

config interface
        option enabled 'yes'
        option interface 'wan'
        option ssm 'yes'
        option igmp 'no'
root@VA_router:/etc/config1# uci show pimd
pimd.pimd=routing
pimd.pimd.enabled=yes
pimd.@interface[0]=interface
pimd.@interface[0].enabled=yes
pimd.@interface[0].interface=lan
pimd.@interface[0].ssm=yes
pimd.@interface[0].igmp=yes
pimd.@interface[1]=interface
```

```
pimd.@interface[1].enabled=yes
pimd.@interface[1].interface=wan
pimd.@interface[1].ssm=yes
pimd.@interface[1].igmp=no
```

Name	Type	Required	Default	Description
enabled	Boolean	Yes	No	Enable PIM and IGMP operation globally.
enabled	Boolean	Yes	No	Enable PIM and IGMP on interface
interface	Interface	Yes	Blank	Specify which interface to apply the settings on
ssm	Boolean	Yes	No	Enable PIM SSM on interface
igmp	Boolean	Yes	No	Enable IGMP on interface

To change any of the above values use uci set command

33 Dynamic Multipoint Virtual Private Network (DMVPN)

Dynamic Multipoint Virtual Private Network (DMVPN) is a scalable method of creating VPN IPSec Networks. DMVPN is a suite of three protocols: NHRP, mGRE and IPSec, used to dynamically create VPN tunnels between different endpoints in the network without having to pre-configure each device with VPN details of the rest of endpoints in the network.

33.1 The advantage of using DMVPN

- Using DMVPN eliminates the need of IPSec configuration to the physical interface. This reduces the number of lines of configuration required for a VPN development. For example, for a 1000-site deployment, DMVPN reduces the configuration effort at the HUB from 3900 lines to 13.
- Adding new peers (spokes) to the VPN requires no changes at the HUB.
- Better scalability of the network.
- Dynamic IP addresses can be used at the peers' site.
- Spokes can be connected in private or public network.
- NHRP NAT extension allows spoke-to-spoke tunnels to be built, even if one or more spokes is behind a Network Address Translation (NAT) device.
- New HUBs can be added to the network to improve the performances and reliability.
- Ability to carry multicast and main routing protocols traffic (RIP, OSPF, BGP).
- DMVPN can be deployed using Activator, the Virtual Access automated provisioning system.
- Simplifies branch communications by enabling direct branch to branch connectivity.
- Simplifies configuration on the spoke routers. The same IPSec template configuration is used to create spoke-to-hub and spoke-to-spoke VPN IPSec tunnel.
- Improves business resiliency by preventing disruption of business-critical applications and services by incorporating routing with standards-based IPsec technology.

33.2 DMVPN scenarios

Scenario 1: Spoke1, Spoke2 and a hub are in the same public or private network

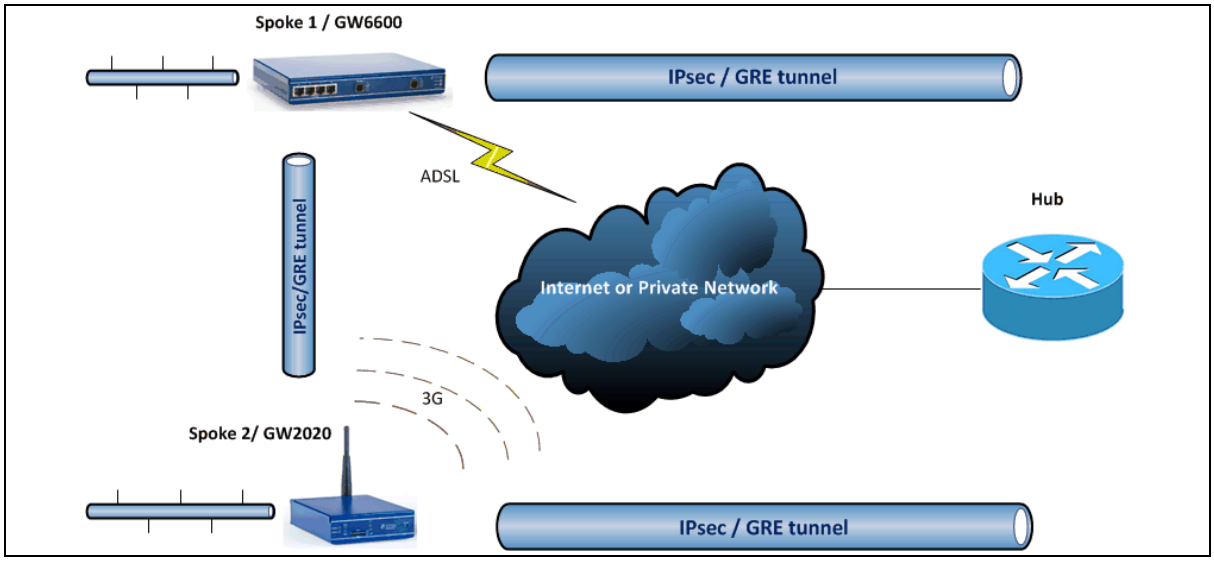


Figure 78: Network diagram for DMVPN spoke to spoke

- Spoke1 and Spoke2 connect on their WAN interface: ADSL, 3G and initiate main mode IPSec in transport mode to the hub.
- After an IPSec tunnel is established, spokes register their NHRP membership with the hub.
- GRE tunnels come up.
- Hub cache the GRE tunnel and real IP addresses of each spoke.
- When Spoke1 wants to talk to Spoke2, it sends an NHRP Resolution Request to the hub.
- The hub checks its cache table and forwards that request to Spoke2.
- Spoke2 caches Spoke1's GRE and real IP address and sends an NHRP Resolution Reply via the hub.
- Spoke1 receives an NHRP resolution reply and updates its NHRP table with Spoke2 information. Then it initiates VPN IPsec connection to Spoke2.
- When an IPsec tunnel is established, Spoke1 and Spoke2 can send traffic directly to each other.

Scenario 2: Spoke1 is in a private (NAT-ed) network, Spoke2 and hub are in public network

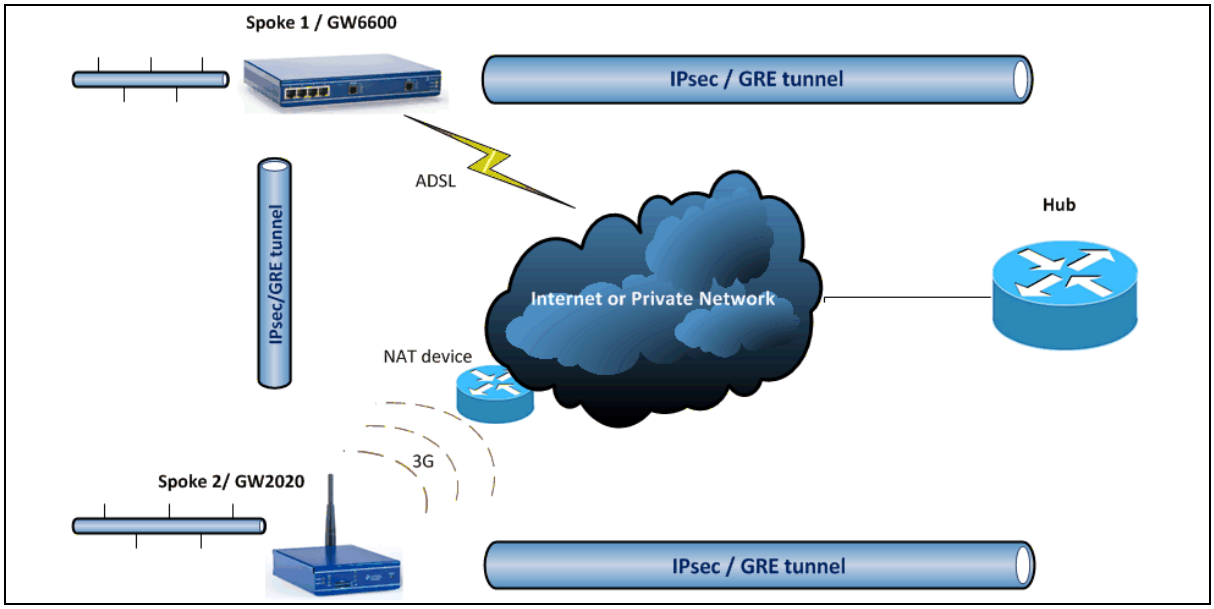


Figure 79: Network diagram for DMVPN spoke behind NAT

- Spoke1 sends an NHRP registration request to the Hub.
- Hub receives this request and compares the source tunnel address of the Spoke with the source of the packet.
- Hub sends an NHRP registration reply with a NAT extension to Spoke1.
- The NAT extension informs Spoke1 that it is behind the NAT-ed device.
- Spoke1 registers its pre- and post-NAT address.
- When Spoke1 wants to talk to Spoke2, it sends an NHRP Resolution Request to the hub.
- Hub checks its cache table and forwards that request to Spoke2.
- Spoke2 caches Spoke1's GRE pre- and post-NAT IP address and sends an NHRP Resolution Reply via the hub.
- Spoke1 receives the NHRP resolution reply and updates its NHRP table with Spoke2 information. It initiates a VPN IPSec connection to Spoke2.
- When the IPSec tunnel is established, Spoke1 and Spoke2 can send traffic directly to each other.
- Note: If an IPSec tunnel fails to be established between the Spokes then packets between the Spokes are sent via the hub.

33.3 Configuring DMVPN via the web interface

Before configuring DMVPN, you must first configure a GRE interface. Read the previous section,'GRE interfaces'.

33.3.1 Configuring IPSec for DMVPN

This section explains how to configure VPN IPSec specifically for DMVPN. For more information on general VPN IPSec configuration, read 'Configuring IPSec' in the GW6600 User Manual.

Access the router's web Interface by typing 192.168.100.1 into your browser.

Type in the username: **root**

Type in the password: **admin**. The Status page appears.

In the top menu click **Services -> IPSec**. The strongSwan IPSec VPN page appears.

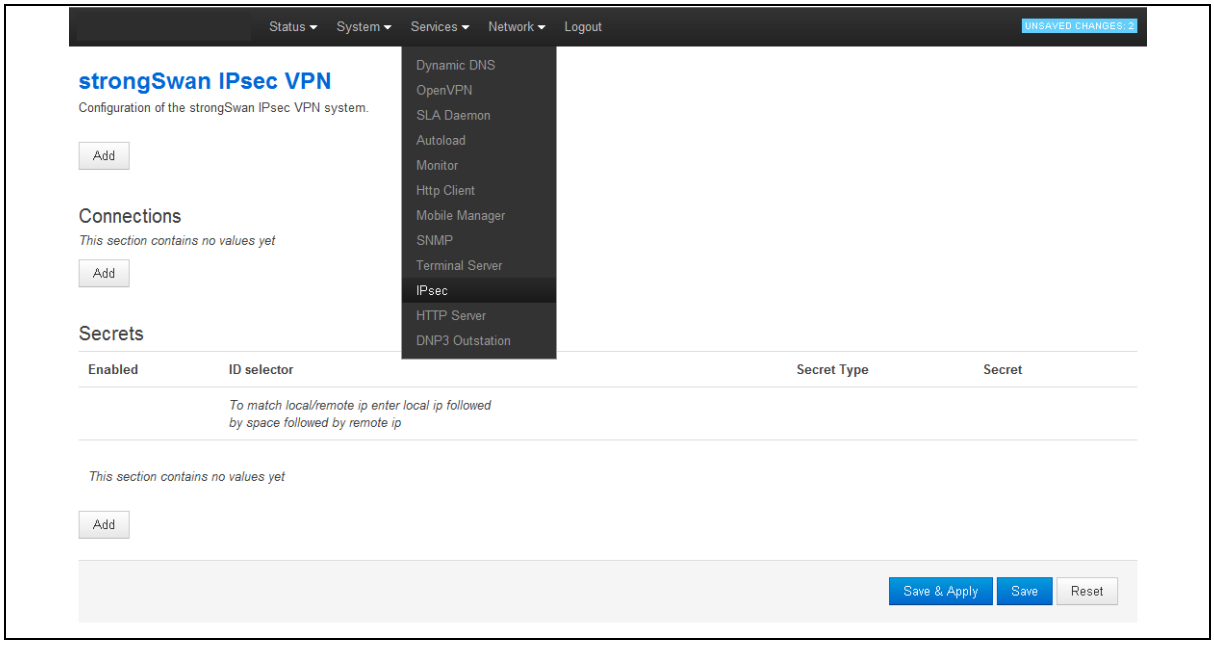


Figure 80: The strongSwan IPSec VPN page

Click the first **Add** button. The strongSwan status now shows an Enabled field that is checked.

strongSwan IPsec VPN
Configuration of the strongSwan IPsec VPN system.
Delete
Enable StrongSwan IPsec
Strict CRL Policy
no
Defines if a fresh CRL must be available in order for the peer authentication based on RSA signatures to succeed. IKEv2 additionally recognizes 'ifuri' which reverts to 'yes' if at least one CRL URI is defined and to 'no' if no URI is known.
Unique IDs
yes
Whether a particular participant ID should be kept unique, with any new (automatically keyed) connection using an ID from a different IP address deemed to replace all old ones using that ID. Participant IDs normally are unique, so a new (automatically-keyed) connection using the same ID is almost invariably intended to replace an old one. The IKEv2 daemon also accepts the value 'replace' which is identical to 'yes' and the value 'keep' to reject new IKE SA setups and keep the duplicate established earlier.
Cache CRLs
CRLs fetched via HTTP or LDAP will be cached.
Debug
none
Connections
This section contains no values yet
Add

Figure 81: strongSwan IPSec enabled

Name	Type	Required	Default	Description
Enable Strongswan IPsec	Boolean	Yes	Blank	Enable Strongswan IPsec
Strict CRL Policy	Dropdown menu	Yes	No	Defines if fresh certificate revocation list (CRL) must be available.
Unique IDs	Dropdown menu	Yes	Yes	Whether a particular participant ID should be kept unique.
Cache CRLs	Boolean	No	Blank	CRLs fetched via HTTP or LDAP will be cached.
Debug	Dropdown menu	No	None	Specifies if IPsec debug should be enabled

Table 17: strongSwan IPSec VPN fields and their descriptions

In the Unique IDs drop down menu, select **Yes**. The Connections settings fields appear.

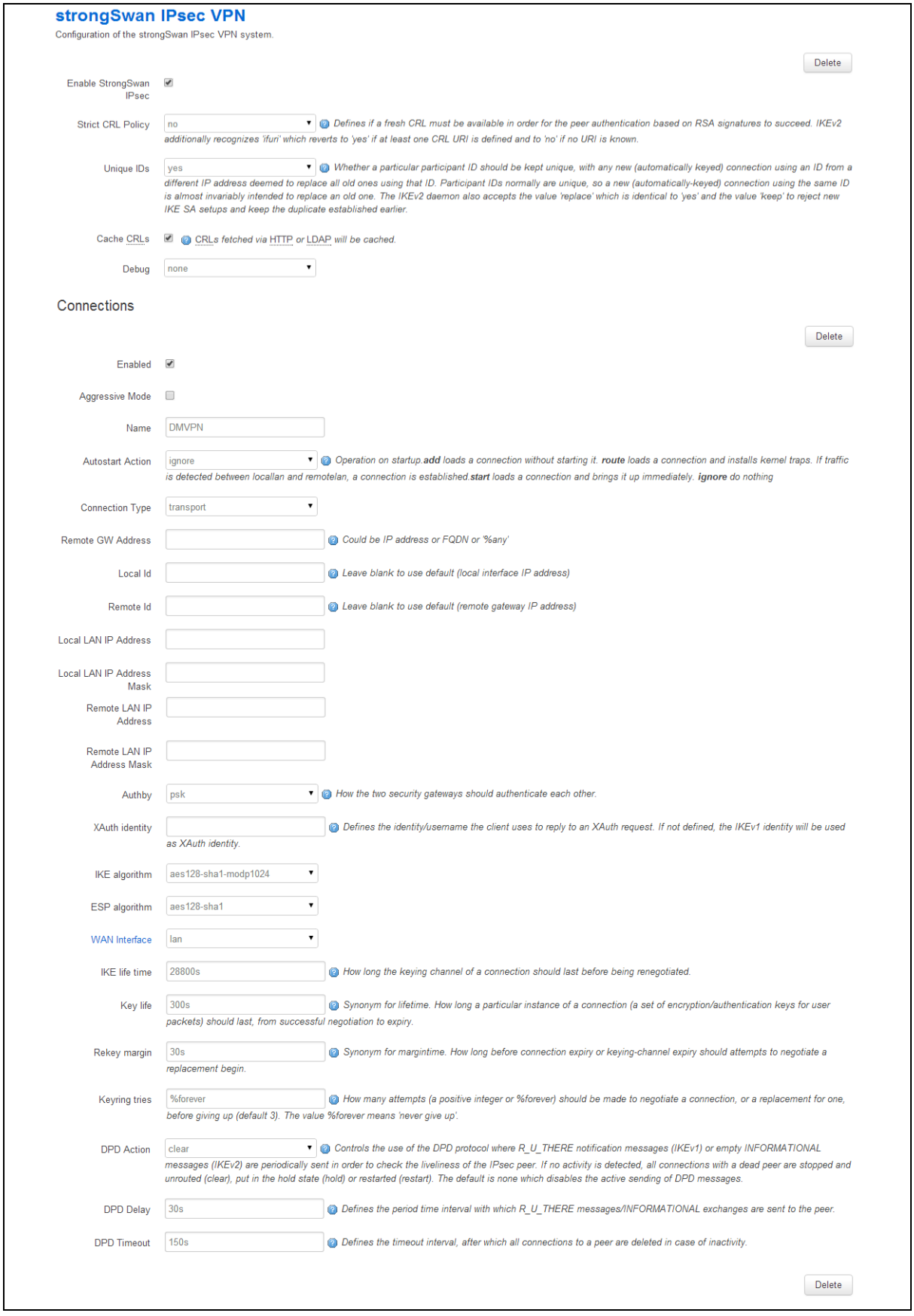

strongSwan IPsec VPN
Configuration of the strongSwan IPsec VPN system.
Delete
Enable StrongSwan IPsec
Strict CRL Policy
no
Defines if a fresh CRL must be available in order for the peer authentication based on RSA signatures to succeed. IKEv2 additionally recognizes 'ifuri' which reverts to 'yes' if at least one CRL URI is defined and to 'no' if no URI is known.
Unique IDs
yes
Whether a particular participant ID should be kept unique, with any new (automatically keyed) connection using an ID from a different IP address deemed to replace all old ones using that ID. Participant IDs normally are unique, so a new (automatically-keyed) connection using the same ID is almost invariably intended to replace an old one. The IKEv2 daemon also accepts the value 'replace' which is identical to 'yes' and the value 'keep' to reject new IKE SA setups and keep the duplicate established earlier.
Cache CRLs
CRLs fetched via HTTP or LDAP will be cached.
Debug
none
Connections
Delete
Enabled
Aggressive Mode
Name
DMVPN
Autostart Action
ignore
Operation on startup.add loads a connection without starting it. route loads a connection and installs kernel traps. If traffic is detected between locallan and remotelan, a connection is established.start loads a connection and brings it up immediately. ignore do nothing
Connection Type
transport
Remote GW Address
Could be IP address or FQDN or '%any'
Local Id
Leave blank to use default (local interface IP address)
Remote Id
Leave blank to use default (remote gateway IP address)
Local LAN IP Address
Local LAN IP Address Mask
Remote LAN IP Address
Remote LAN IP Address Mask
Authby
psk
How the two security gateways should authenticate each other.
XAuth identity
Defines the identity/username the client uses to reply to an XAuth request. If not defined, the IKEv1 identity will be used as XAuth identity.
IKE algorithm
aes128-sha1-modp1024
ESP algorithm
aes128-sha1
WAN Interface
lan
IKE life time
28800s
How long the keying channel of a connection should last before being renegotiated.
Key life
300s
Synonym for lifetime. How long a particular instance of a connection (a set of encryption/authentication keys for user packets) should last, from successful negotiation to expiry.
Rekey margin
30s
Synonym for margintime. How long before connection expiry or keying-channel expiry should attempts to negotiate a replacement begin.
Keyring tries
%forever
How many attempts (a positive integer or %forever) should be made to negotiate a connection, or a replacement for one, before giving up (default 3). The value %forever means 'never give up'.
DPD Action
clear
Controls the use of the DPD protocol where R_U_THERE notification messages (IKEv1) or empty INFORMATIONAL messages (IKEv2) are periodically sent in order to check the liveliness of the IPsec peer. If no activity is detected, all connections with a dead peer are stopped and unrouted (clear), put in the hold state (hold) or restarted (restart). The default is none which disables the active sending of DPD messages.
DPD Delay
30s
Defines the period time interval with which R_U_THERE messages/INFORMATIONAL exchanges are sent to the peer.
DPD Timeout
150s
Defines the timeout interval, after which all connections to a peer are deleted in case of inactivity.
Delete

Figure 82: The strongSwan IPSec VPN page

Name	Type	Required	Default	Description
Enabled	Checkbox	yes	Unchecked	Globally enables IPSec on the router.
Aggressive mode	Checkbox	yes	Unchecked	Globally enables Aggressive mode on a router.
Name	String	Yes	Blank	Specifies a name for the tunnel.
Autostart Action	Dropdown Menu	Yes	Ignore	Specifies how the tunnel is initiated. Start On startup Route When traffic routes this way. Add Loads a connection without starting it. Ignore Ignores the connection.
Connection Type	Dropdown Menu	Yes	tunnel	Defines whether the connection is in tunnel or transport mode.
Remote GW address	IP address	Yes	None	Sets the public IP address of a remote peer.
Local Id	string	Yes	None	Defines the local peer identifier.
Remote Id	String	Yes	None	Sets the remote peer identifier.
Local LAN IP Address	String	Yes	None	Defines the local IP of LAN.
Local LAN IP Address Mask	String	Yes	None	Defines the local Mask of LAN.
Remote LAN IP Address	String	Yes	None	Defines the Remote IP of LAN.
Remote LAN IP Address Mask	String	Yes	None	Defines the Remote Mask of LAN.
Authby	Dropdown Menu	Yes	psk	Defines authentication method. Available options, psk, xauthpsk.
XAuth identity	String	No	None	Defines the identity/username the client uses to reply to an XAuth request. If not defined, the IKEv1 identity will be used as XAuth identity.
IKE algorithm	Dropdown Menu	Yes	aes128-sha1-modp2048, 3des-sha1-modp1536	Specifies the IKE algorithm to use. The format is: encAlgo-authAlgo-DHGroup encAlgo: 3des, aes, serpent, twofish, blowfish authAlgo: md5, sha, sha2 DHGroup: modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, modp8192
ESP algorithm	Dropdown Menu	Yes	aes128-sha1, 3des-sha1	Specifies the esp algorithm to use. The format is:

				encAlgo-authAlgo-PFSGroup encAlgo: 3des, aes, serpent, twofish, blowfish authAlgo: md5, sha, sha2 DHGroup: modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, modp8192 For example: aes128-sha1-modp1536. If no DH group is defined then PFS is disabled.
WAN interface	Dropdown Menu	Yes	None	Defines the WAN interface used by this tunnel.
IKE life time	Integer	Yes	3h	Specifies how long the keying channel of a connection (ISAKMP or IKE SA) should last before being renegotiated. Syntax: timespec: 1d, 2h, 25m, 10s.
Key life	Integer	Yes	1h	Specifies how long a particular instance of a connection, a set of encryption/authentication keys for user packets, should last, from successful negotiation to expiry. Normally, the connection is renegotiated, via the keying channel, before it expires (see rekeymargin). Syntax: timespec: 1d, 2h, 25m, 10s.
Rekey margin	Integer	Yes	9m	Margintime. Defines how long before a connection expiry or keying-channel expiry should begin to attempt to negotiate a replacement.
Keyring tries	String	Yes	3	Specifies how many attempts a positive integer or %forever should be made to negotiate a connection, or a replacement for one, before giving up. The value %forever means 'never give up'. It is only relevant locally; the other end does not need to agree on it.
DPD Action	Dropdown Menu	Yes	None	Valid values are none, clear, hold and restart. None Disables dead peer detection. Clear Clears down the tunnel if a peer does not respond. Reconnects

				when traffic brings the tunnel up. Hold Clears down the tunnel and bring up as soon as the peer is available. Restart Restarts DPD when no activity is detected.
DPD Delay	Integer	Yes	None	Defines the period time interval with which R_U_THERE messages/INFORMATIONAL exchanges are sent to the peer. These are only sent if no other traffic is received. Syntax: timespec: 1d, 2h, 25m, 10s.
DPD Timeout	Integer	Yes	150s	Defines the timeout interval, after which all connections to a peer are deleted in case of inactivity. Syntax: timespec: 1d, 2h, 25m, 10s.

Table 18: Connections fields for strongSwan IPSec VPN

From the Name field, type the **Connection Name**.

From the Autostart Action drop down menu, select **Ignore**.

From the Connection Type drop down menu, select **transport**.

From the Authby dropdown menu, select **psk**.

From the IKE algorithm dropdown menu, select the **encryption**, **hash algorithm** and **DH group**.

From the ESP algorithm dropdown menu, select the **encryption** and **hash algorithm**.

From the WAN Interface dropdown menu select the interface that is used to transmit IPSec packets.

In the IKE life time field, type the **Ike life time value**.

In the Key life field, type the **Key life value**.

In the Keying tries field, type a **%forever** value.

From the DPD Action drop down menu, select **clear**.

In the DPD Delay field, type a **DPD delay** value.

In the DPD Timeout field, type a relevant value.

At the bottom of the Secrets section, click **Add**.

© Virtual Access 2015

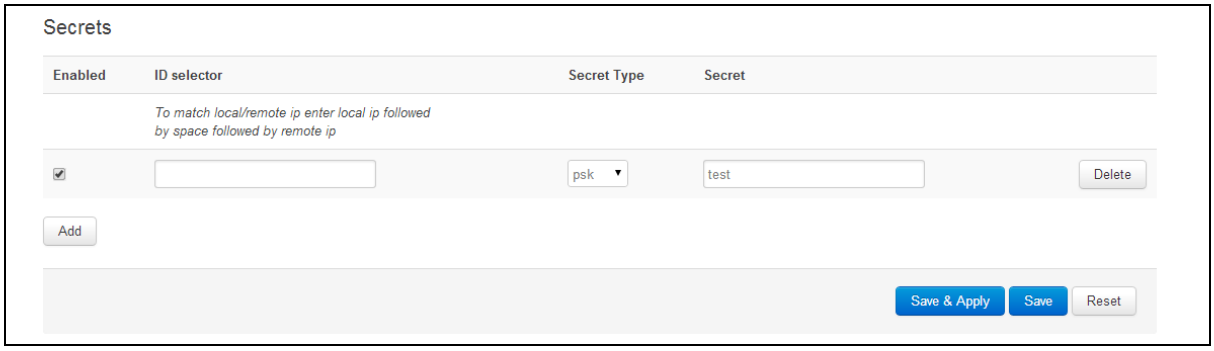


Figure 83: The secrets section

Select **Enabled**.

From the dropdown menu under Secret Type, select **psk**.

In the field beneath Secret, type the **psk password**.

Click **Save**.

33.4 DMVPN hub settings

In the top menu, select **Network -> DMVPN**. The DMVPN page appears.

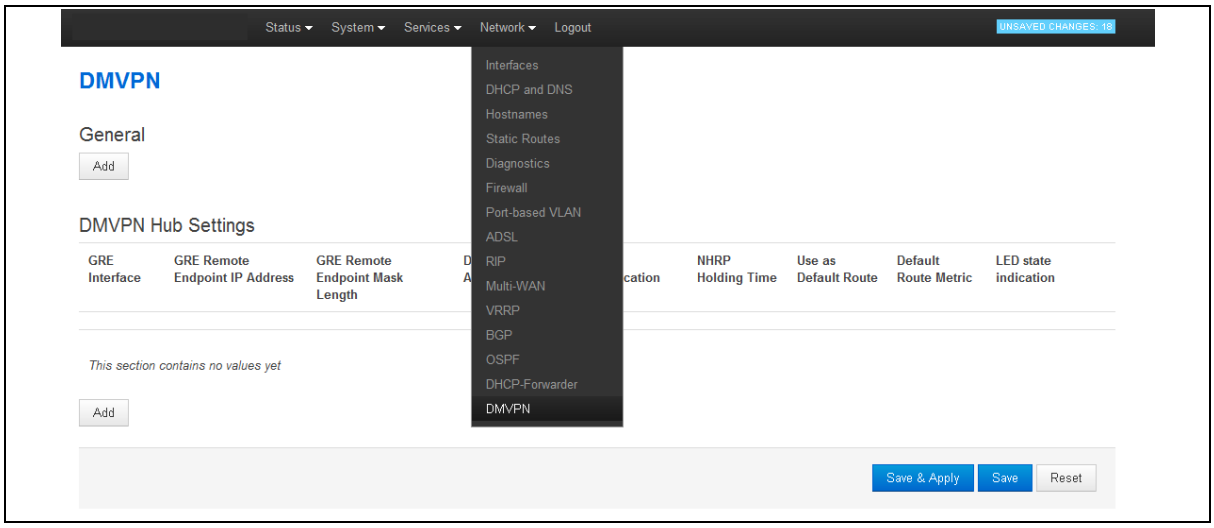


Figure 84: The DMVPN page

Under DMVPN General, click **Add**. The following page appears.

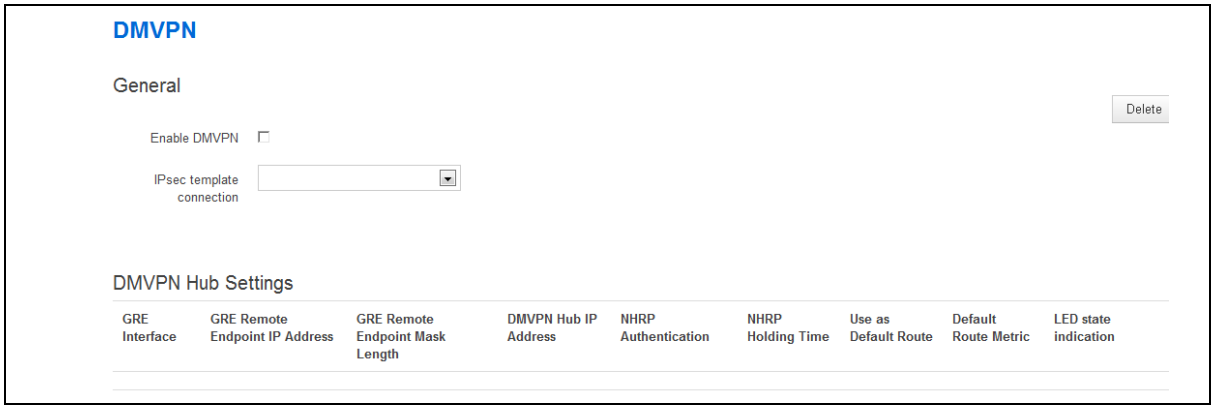


Figure 85: The DMVPN general section

Check **Enable DMVPN**.

From the IPSec template connection drop down menu, provide the **name of the IPsec connection**.

In the DMVPN Hub Settings section, click **Add**. The fields required to configure the parameters relative to the DMVPN Hub appear. These are used for the DMVPN tunnels, such as GRE tunnels, GRE tunnel remote IP, DMVPN Hub IP and password.

Name	Type	Required	Default	Description
GRE Interface	Dropdown list	Yes	Blank	Specifies which GRE interface will be used with this DMVPN configuration.
GRE Remote Endpoint IP Address	IP address	Yes	Blank	Configures the GRE IP address of the hub.
DMVPN Hub IP Address	IP address	Yes	Blank	Configures the physical IP address for the DMVPN hub.
NHRP Authentication	Numeric value	Yes	Blank	Enables authentication on NHRP. The password will be applied in plaintext to the outgoing NHRP packets. Maximum length is 8 characters.
NHRP Holding Time	Integer	Yes	Blank	Timeout for cached NHRP requests.

Table 19: DMVPN hub fields and their descriptions

33.5 UCI interface

33.5.1 IPSec configuration using CLI

You can configure IPSec (strongSwan package) through CLI using the UCI command suite.

Configuration files are stored at:

/etc/config/strongswan

To view the configuration file, use uci show strongswan or uci export strongswan commands.

```
root@GWxxxx:~# uci show strongswan
strongswan.general=general
strongswan.general.enabled=yes
strongswan.general.strictcrlpolicy=no
strongswan.general.uniqueids=yes
strongswan.general.cachecrls=yes
strongswan.general.nattraversal=yes
strongswan.@connection[0]=connection
strongswan.@connection[0].enabled=yes
strongswan.@connection[0].name=DMVPN
strongswan.@connection[0].type=transport
strongswan.@connection[0].localproto=gre
strongswan.@connection[0].remoteproto=gre
strongswan.@connection[0].ike=3des-md5-modp1024
strongswan.@connection[0].esp=aes128-sha1
strongswan.@connection[0].waniface=wan
strongswan.@connection[0].auto=ignore
strongswan.@connection[0].ikelifetime=28800s
strongswan.@connection[0].keylife=300s
strongswan.@connection[0].rekeymargin=30s
strongswan.@connection[0].keyingtries=%forever
strongswan.@connection[0].dpdaction=hold
strongswan.@connection[0].dpddelay=30s
strongswan.@connection[0].dpdtimeout=150s
strongswan.@secret[0]=secret
strongswan.@secret[0].enabled=yes
strongswan.@secret[0].secrettype=psk
strongswan.@secret[0].secret=secret
```

```
uci export strongswan

package strongswan

config general 'general'
        option enabled 'yes'
        option strictcrlpolicy 'no'
        option uniqueids 'yes'
        option cachecrls 'yes'
        option nattraversal 'yes'

config connection
        option enabled 'yes'
        option name 'DMVPN'
        option type 'transport'
        option localproto 'gre'
        option remoteproto 'gre'
        option ike '3des-md5-modp1024'
        option esp 'aes128-sha1'
        option waniface 'wan'
        option auto 'ignore'
        option ikelifetime '28800s'
        option keylife '300s'
        option rekeymargin '30s'
        option keyingtries '%forever'
        option dpdaction 'hold'
        option dpddelay '30s'
        option dpdtimeout '150s'

config secret
        option enabled 'yes'
        option secrettype 'psk'
        option secret 'secret'
```

33.6 Configuring DMVPN using CLI

You can configure DMVPN through CLI using the UCI command suite.

Configuration files are stored at:

/etc/config/dmvpn

To view the configuration file, use uci show dmvpn or uci export dmvpn commands.

```
uci export dmvpn

package dmvpn

config general-settings 'common'
        option enabled 'yes'
        option ipsec_template_name 'DMVPN'

config interface
        option holding_time '60'
        option gre_interface 'GRE'
        option gre_endpoint_ip '11.11.11.1'
        option gre_endpoint_mask_length '29'
        option nhs_ip '192.168.100.1'
        option cisco_auth 'test'

uci show dmvpn

dmvpn.common=general-settings
dmvpn.common.enabled=yes
dmvpn.common.ipsec_template_name=DMVPN
dmvpn.@interface[0]=interface
dmvpn.@interface[0].holding_time=60
dmvpn.@interface[0].gre_interface=GRE
dmvpn.@interface[0].gre_endpoint_ip=11.11.11.1
dmvpn.@interface[0].gre_endpoint_mask_length=29
dmvpn.@interface[0].nhs_ip=192.168.100.1
dmvpn.@interface[0].cisco_auth=test
```

To change any of the above values, use uci set command.

34 Event system

Virtual Access routers feature an event system.

The event system allows you to configure the router's information for efficient control and management of devices.

This section explains how the event system works and how to configure it using via UCI.

34.1 Implementation of the event system

The event system is implemented by the va_eventd application.

The va_eventd application defines three types of object:

Forwardings	Rules that define what kind of events should be generated. For example you might want an event to be created when an IPSec tunnel comes up or down.
Targets	Define the targets to send the event to. The event may be sent to a target via a syslog message, a snmp trap or email.
Connection testers	Define methods to test the target is reachable. IP connectivity to a server and link state may be checked prior to sending events.

For example, if you want to configure a snmp trap to be sent when an IPSec tunnel comes up, you will need to:

- Define a forwarding rule for IPSec tunnel up events
- Set an SNMP manager as the target
- Optionally using a connection tester to ensure the SNMP manager is reachable

34.2 Supported events

Events have a class, a name and a severity. These three properties are used to fine tune which events to report.

34.3 Supported targets

The table below describes the targets currently supported.

Target	Description
Syslog	Event sent to syslog server
Email	Event sent via email

SNMP	Event sent via SNMP trap
Exec	Command executed when event occurs

Table 27: Event system - supported targets

The attributes of a target vary significantly depending on its type.

34.4 Supported connection testers

The table below describes the methods to test a connection that are currently supported:

Type	Description
link	Checks if the interface used to reach the target is up
ping	Pings the target. It then assumes there is connectivity during a configurable amount of time

Table 28: Event system - supported connection tester methods

34.5 Configuring the event system via the web interface

Configuring the event system via the web interface is not currently supported.

34.6 Configuring the event system via UCI

The event system configuration files are stored on:

/etc/config/va_eventd

The configuration is composed of a main section and as many forwardings, targets and connection testers as required.

34.6.1 Main section

```
config va_eventd main
       option enabled yes
       option event_queue_file '/tmp/event_buffer'
       option event_queue_size 128K
```

The table below describes main event system parameters:

Name	Type	Required	Default	Description
enabled	Boolean	Yes	Yes	Enable the event system
event_queue_file	Filename	Yes	/tmp/event_buffer	File where the events will be stored before being processed
event_queue_size	String	Yes	128K	Maximum size of the event queue

Table 29: Event system - global settings description

34.6.2 Forwardings

```
config forwarding
        option enabled no
        option className ethernet
        option eventName LinkUp
        option severity warning-critical
        option target syslog1
```

The table below describes event system forwarding parameters.

Name	Type	Required	Default	Description
enabled	Boolean	Yes	Yes	Enable the event generation
className	String	No	None	Only generate events with the given className
eventName	String	No	None	Only generate events with the given className and the given eventName
severity	String	No	None	Only generate events with a severity in the severity range
target	String	Yes	None	Target to send the event to

Table 30: Event system - forwarding rules settings description

Severity must be a range in the form severity1-severity2. Severity1 and severity2 are a level among debug, info, notice, warning, error, critical, alert, and emergency.

34.6.3 Connection testers

There are two types of connection testers:

- ping connection tester, and
- link connection tester.

34.6.3.1 Ping connection tester

A ping connection tester tests that a connection can be established by sending pings.

If successful, the event system assumed the connection is valid for a configurable amount of time.

```
config conn_tester
	option name pinger
	option enabled yes
	option type ping
	option ping_dest_addr 192.168.0.1
	option ping_source eth0
	option ping_success_duration_sec 60
```

The table below describes ping connection tester parameters.

Name	Type	Required	Default	Description
name	String	Yes	None	Name of the target to be used in the target section
enabled	Boolean	Yes	Yes	Enable this connection tester
type	String	Yes	Ping	Must be ping for a ping connection tester
ping_dest_addr	IP Address	Yes	None	IP Address to ping
ping_source	IP Address or String	No	None	Source IP Address of the pings It can also be an interface name
ping_success_duration_sec	Time in secs	Yes	None	Time the target is considered up for after a successful ping

Table 31: Event system – ping connection tester settings description

34.6.3.2 Link connection tester

A link connection tester tests a connection by checking the status of the interface being used.

```
config conn_tester
	option name t1
	option enabled 1
	option type link
	option link_iface eth0
```

© Virtual Access 2015

The table below describes link connection tester parameters.

Name	Type	Required	Default	Description
name	String	Yes	None	Name of the target to be used in the target section
enabled	Boolean	Yes	Yes	Enable this connection tester
type	String	Yes	Link	Must be link for a link connection tester
link_iface	String	Yes	None	Interface name to check

Table 32: Event system – link connection tester settings description

34.6.4 Supported targets

There are four possible targets.

- Syslog target
- Email target
- SNMP target
- Exec target

34.6.4.1 Syslog target

When a syslog target receives an event, it sends it to the configured syslog server.

```
config target
       option name syslog1
       option enabled yes
       option type syslog
       option target_addr "192.168.0.1:514"
       option conn_tester t1
```

The table below describes syslog target parameters.

Name	Type	Required	Default	Description
name	String	Yes	None	Name of the target to be used in the forwarding section
enabled	Boolean	Yes	Yes	Enable this target
type	String	Yes	Syslog	Must be syslog for a syslog target
target_addr	IP Address:Port	Yes	None	IP Address and Port number to send the syslog message to. If no port is given, 514 is assumed
conn_tester	String	No	None	Name of the connection tester to use for this target

Table 33: Event system – syslog target settings description

34.6.4.2 Email target

When an email target receives an event, it sends it to the configured email address.

```
config target
	option name email
	option enabled yes
	option type email
	option conn_tester pinger
	option smtp_addr "smtp.site.com:587"
	option smtp_user 'john_smith@site.com'
	option smtp_password 'secret word'
	option use_tls 'yes'
	option tls_starttls 'yes'
	option tls_forcessl3 'yes'
	option timeout_sec "10"

	option from x@example.com
	option to y@example.com
	option subject_template "%{severityName} %{eventName}!!!"
	option body_template "%{eventName} (%{class}.%{subclass}) happened!"
	option conn_tester 'smtp_server'
```

The table below describes email target parameters.

Name	Type	Required	Default	Description
name	String	Yes	None	Name of the target to be used in the forwarding section
enabled	Boolean	Yes	Yes	Enable this target
type	String	Yes	Email	Must be email for a syslog target
smtp_addr	IP Address:Port	Yes	None	IP Address and port of the SMTP server to use.
smtp_user	String	No	None	Username for smtp authentication
smtp_password	String	No	None	Password for smtp authentication
use_tls	Boolean	No	No	Enable tls support
tls_starttls	Boolean	No	No	Enable starttls support
tls_forcessl3	Boolean	No	No	Force SSLv3 for TLS
timeout_sec	Time in secs	No	No	Email send timeout
from	Email address	Yes	No	Source email address
to	Email address	Yes	No	Destination email address

subject_template	String	No	None	Template to use for the email subject
body_template	String	No	None	Template to use for the email body
conn_tester	String	No	None	Name of the connection tester to use for this target

Table 34: Event system – email target settings description

34.6.4.3 SNMP target

When a SNMP target receives an event, it sends it in a trap to the configured SNMP manager.

```
config target
	option name snmp
	option enabled yes
	option type snmptrap
	option community public
	option target_addr 192.168.0.1
	option agent_addr 192.168.0.4
	option conn_tester pinger
```

The table below describes SNMP target parameters.

Name	Type	Required	Default	Description
name	String	Yes	None	Name of the target to be used in the forwarding section
enabled	Boolean	Yes	Yes	Enable this target
type	String	Yes	snmptrap	Must be snmptrap for a snmp target
Community	String	Yes	None	Community name to use to send the trap
target_addr	IP Address	Yes	None	IP Address of a the SNMP Manager
agent_addr	IP Address	No	None	IP Address to use as the trap source IP address
conn_tester	String	No	None	Name of the connection tester to use for this target

Table 35: Event system – snmp target settings description

34.6.4.4 Exec target

When an exec target receives an event, it executes a shell command.

```
config target
       option name logit
       option enabled yes
       option type exec
       option cmd_template "logger -t eventer %{eventName}"
```

The table below describes exec target parameters.

Name	Type	Required	Default	Description
name	String	Yes	None	Name of the target to be used in the forwarding section
enabled	Boolean	Yes	Yes	Enable this target
type	String	Yes	exec	Must be exec for a exec target
cmd_template	String	Yes	None	Template of the command to execute

Table 36: Event system – exec target settings description

34.6.5 Example and export

As an example, the event system is configured to:

- Forward the “l2tp” event “CannotFindTunnel” with a severity between debug and critical to a syslog server
- Forward all “mobile” events with a severity between notice and critical to a SNMP trap manager
- Execute “logger -t eventer %{eventName}” when an “Ethernet” event occurs
- Forward all “auth” events via email
- Connection to the SNMP and syslog server is checked by sending pings
- Connection to the smtp server is verified by checking the state of “eth0”

To view the configuration file, enter:

uci export va_eventd

```
root@test:~# uci export va_eventd
package va_eventd

config va_eventd 'main'
        option enabled 'yes'
        option event_queue_file '/tmp/event_buffer'
        option event_queue_size '128K'
```

```
config forwarding
        option enabled 'yes'
        option className 'l2tp'
        option eventName 'CannotFindTunnel'
        option severity 'debug-critical'
        option target 'syslog'

config forwarding
        option enabled 'yes'
        option className 'mobile'
        option severity 'notice-critical'
        option target 'snmp'

config forwarding
        option enabled 'yes'
        option className 'ethernet'
        option target 'logit'

config forwarding
        option enabled 'yes'
        option className 'auth'
        option target 'email'

config conn_tester
        option name 'mon_server'
        option enabled '1'
        option type 'ping'
        option ping_dest_addr '192.168.100.254'
        option ping_source 'eth0'
        option ping_success_duration_sec '10'

config conn_tester
        option name 'smtp_server'
        option enabled '1'
        option type 'link'
        option link_iface 'eth0'
```

```
config target
        option name 'syslog'
        option enabled 'yes'
        option type 'syslog'
        option target_addr '192.168.100.254:514'
        option conn_tester 'mon_server'

config target
        option name 'email'
        option enabled 'yes'
        option type 'email'
        option smtp_addr '89.101.154.148:465'
        option smtp_user 'x@example.com'
        option smtp_password '******'
        option use_tls 'yes'
        option tls_starttls 'no'
        option tls_forcessl3 'no'
        option timeout_sec '10'
        option from 'y@example.com'
        option to 'z@example.com'
        option subject_template '%{severityName} %{eventName}!!!'
        option body_template '%{eventName} (%{class}.%{subclass})
happened!'
        option conn_tester 'smtp_server'

config target
        option name 'snmp'
        option enabled 'yes'
        option type 'snmptrap'
        option community 'public'
        option target_addr '192.168.100.254'
        option agent_addr '192.168.100.1'
        option conn_tester 'mon_server'

config target
        option name 'logit'
        option enabled 'yes'
```

```
        option type 'exec'
        option cmd_template 'logger -t eventer %{eventName}'
```

To view UCI commands, enter:

uci show va_eventd

```
root@test:~# uci show va_eventd
va_eventd.main=va_eventd
va_eventd.main.enabled=yes
va_eventd.main.event_queue_file=/tmp/event_buffer
va_eventd.main.event_queue_size=128K
va_eventd.@forwarding[0]=forwarding
va_eventd.@forwarding[0].enabled=yes
va_eventd.@forwarding[0].className=l2tp
va_eventd.@forwarding[0].eventName=CannotFindTunnel
va_eventd.@forwarding[0].severity=debug-critical
va_eventd.@forwarding[0].target=syslog
va_eventd.@forwarding[1]=forwarding
va_eventd.@forwarding[1].enabled=yes
va_eventd.@forwarding[1].className=mobile
va_eventd.@forwarding[1].severity=notice-critical
va_eventd.@forwarding[1].target=snmp
va_eventd.@forwarding[2]=forwarding
va_eventd.@forwarding[2].enabled=yes
va_eventd.@forwarding[2].className=ethernet
va_eventd.@forwarding[2].target=logit
va_eventd.@forwarding[3]=forwarding
va_eventd.@forwarding[3].enabled=yes
va_eventd.@forwarding[3].className=auth
va_eventd.@forwarding[3].target=email
va_eventd.@conn_tester[0]=conn_tester
va_eventd.@conn_tester[0].name=mon_server
va_eventd.@conn_tester[0].enabled=1
va_eventd.@conn_tester[0].type=ping
va_eventd.@conn_tester[0].ping_dest_addr=192.168.100.254
va_eventd.@conn_tester[0].ping_source=eth0
```

```
va_eventd.@conn_tester[0].ping_success_duration_sec=10
va_eventd.@conn_tester[1]=conn_tester
va_eventd.@conn_tester[1].name=smtp_server
va_eventd.@conn_tester[1].enabled=1
va_eventd.@conn_tester[1].type=link
va_eventd.@conn_tester[1].link_iface=eth0
va_eventd.@target[0]=target
va_eventd.@target[0].name=syslog
va_eventd.@target[0].enabled=yes
va_eventd.@target[0].type=syslog
va_eventd.@target[0].target_addr=192.168.100.254:514
va_eventd.@target[0].conn_tester=mon_server
va_eventd.@target[1]=target
va_eventd.@target[1].name=email
va_eventd.@target[1].enabled=yes
va_eventd.@target[1].type=email
va_eventd.@target[1].smtp_addr=89.101.154.148:465
va_eventd.@target[1].smtp_user=x@example.com
va_eventd.@target[1].smtp_password=******
va_eventd.@target[1].use_tls=yes
va_eventd.@target[1].tls_starttls=no
va_eventd.@target[1].tls_forcessl3=no
va_eventd.@target[1].timeout_sec=10
va_eventd.@target[1].from=y@example.com
va_eventd.@target[1].to=z@example.com
va_eventd.@target[1].subject_template=%{severityName} %{eventName}!!!
va_eventd.@target[1].body_template=%{eventName} (%{class}.%{subclass})
happened!
va_eventd.@target[1].conn_tester=smtp_server
va_eventd.@target[2]=target
va_eventd.@target[2].name=snmp
va_eventd.@target[2].enabled=yes
va_eventd.@target[2].type=snmptrap
va_eventd.@target[2].community=public
va_eventd.@target[2].target_addr=192.168.100.254
va_eventd.@target[2].agent_addr=192.168.100.1
va_eventd.@target[2].conn_tester=mon_server
```

© Virtual Access 2015

```
va_eventd.@target[3]=target
va_eventd.@target[3].name=logit
va_eventd.@target[3].enabled=yes
va_eventd.@target[3].type=exec
va_eventd.@target[3].cmd_template=logger -t eventer %{eventName}
```

35 Configuring SLA reporting on Monitor

35.1 Introduction

This section describes how to configure and view SLA reporting on Monitor, the Virtual Access monitoring system. It also explains how to configure scheduler task that is placed on the router to upload SLA statistics.

The Virtual Access Monitor system provides:

- centralised access to router connectivity status,
- access to advanced router diagnostic tools, and
- access to SLA Report Management.

The SLA Report Manager can build reports from a list of selected routers presenting a range of statistics over extended periods of time, including:

- Availability
- Latency
- Packet loss
- 3G signal strength

35.2 Configuring SLA reporting

To configure SLA reporting on Monitor, you must first add a content template and then build an SLA report based on it. A content template allows you to enable and configure report elements that you can then add to an SLA report.

When you have added a content template, you can then add an SLA report.

35.2.1 Configuring a content template

Click **Settings** on the Monitor home page. The settings page appears.

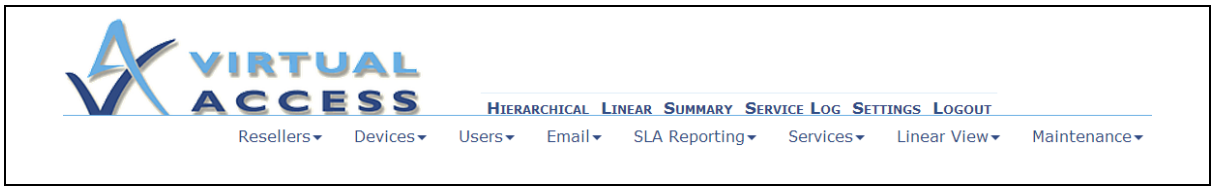


Figure 123: The settings page on Monitor

In the top menu, select **SLA Reporting ->Content Templates**. Then click **Create**. The Add/Edit Content Template page appears.

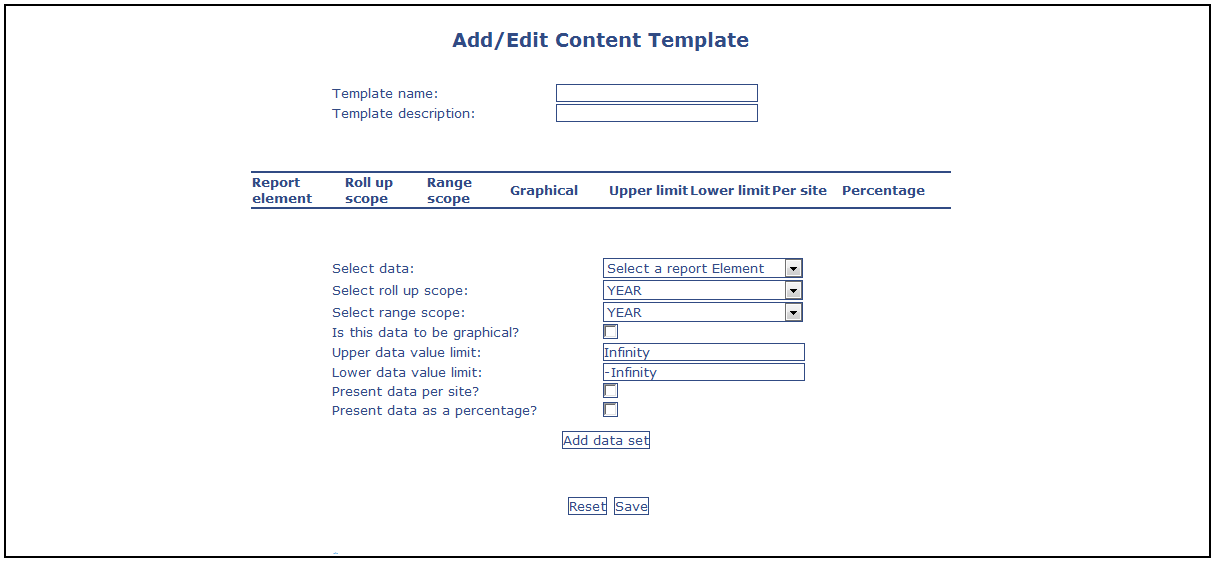


Figure 124: The add/edit content template

Enter a relevant name and description and then add values from the drop-down menu or enter values for the parameters shown in the table below.

Parameter	Description / Default	Options
Select data	Report element to display data on.	Average Latency Average Packet Loss Average Latency Average Availability Average Connection Strength Max Latency Max Packet Loss Max Latency Max Availability Max Connection Strength
Select roll up scope	Scope rollup period	Year Month Week Day Hour Minute Second
Select range scope	Range of scope	Year Month Week Day Hour Minute Second

© Virtual Access 2015

Is this data to be graphical?	To display elements as graphs	Tick or no tick
Upper data value limit	Infinity	Integer
Lower data value limit	-Infinity	Integer
Present data per site?		Tick or no tick
Present data as a percentage?		Tick or no tick

Table 37: Parameters for content template

If you want the data to be displayed as graphical, click the **Is this data to be graphical?** checkbox.

Enter relevant parameters for upper and lower data limits. The default is **+** and **–** infinity.

If you require, click the **Present data per site?** checkbox and the **Present data as a percentage?** checkbox.

You must add the content template parameters for each report element.

The figure below details the settings required for Avg Latency data.

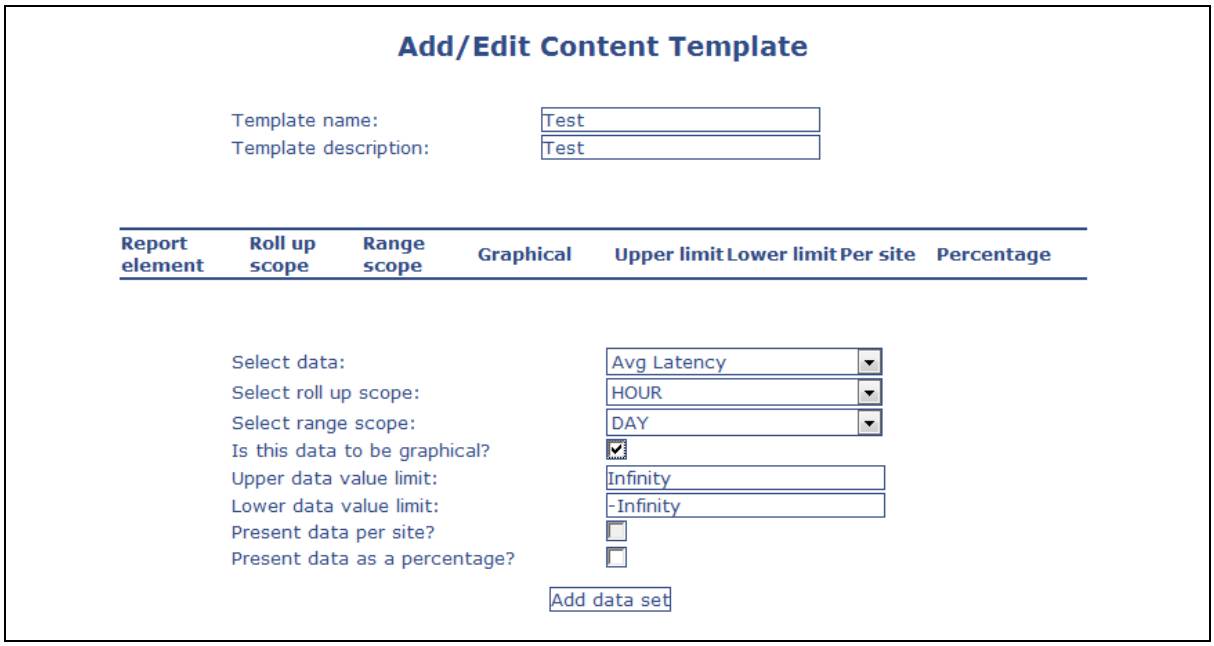


Figure 125: Example of Avg latency parameters

When you have entered all the parameters you require, click **Add data set**.

Repeat the process for Avg Connection strength, Avg Packetloss and Avg Latency.

The template will build as shown in the figure below. The example graphs average latency, connection strength, and packet loss, with a roll up period set per hour and a range scope set per day.

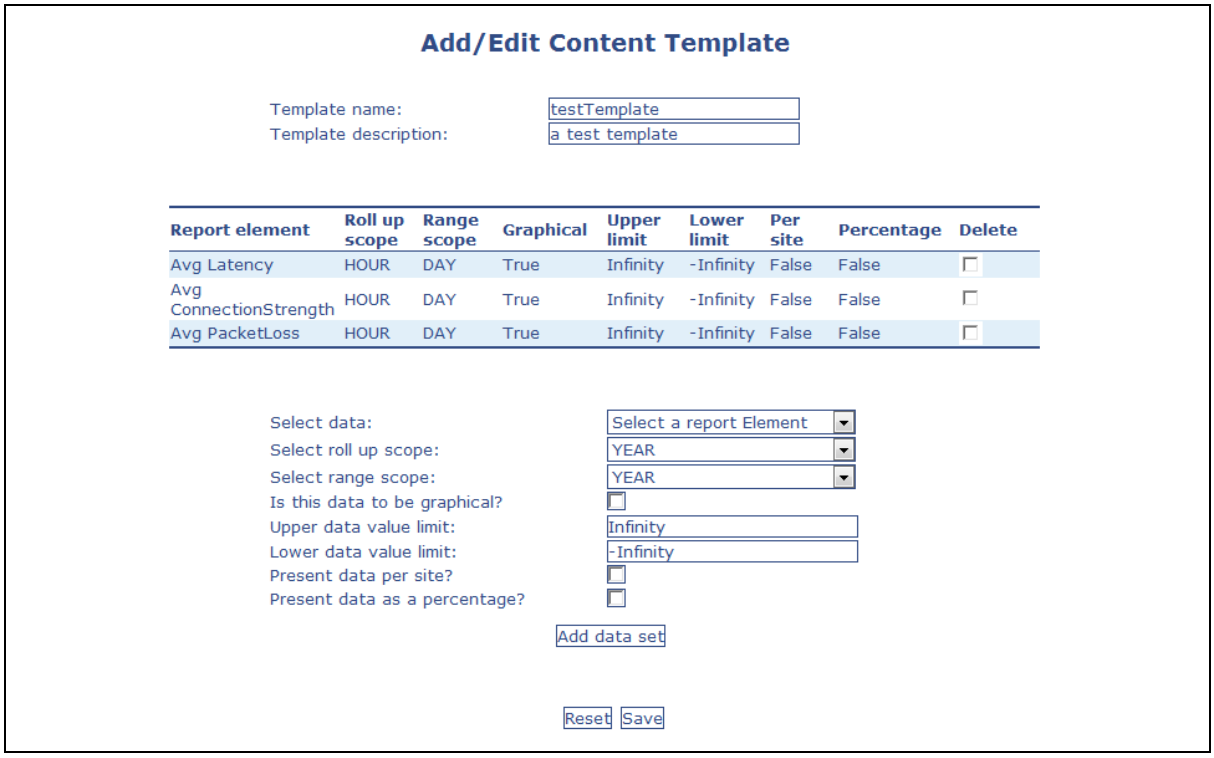


Figure 126: Example content template

35.3 Adding an SLA report

When you have configured a content template, you can add an SLA report.

In the top menu, click **SLA Reporting -> REPORTS**. Then click **Create**. The Add SLA Report page appears.

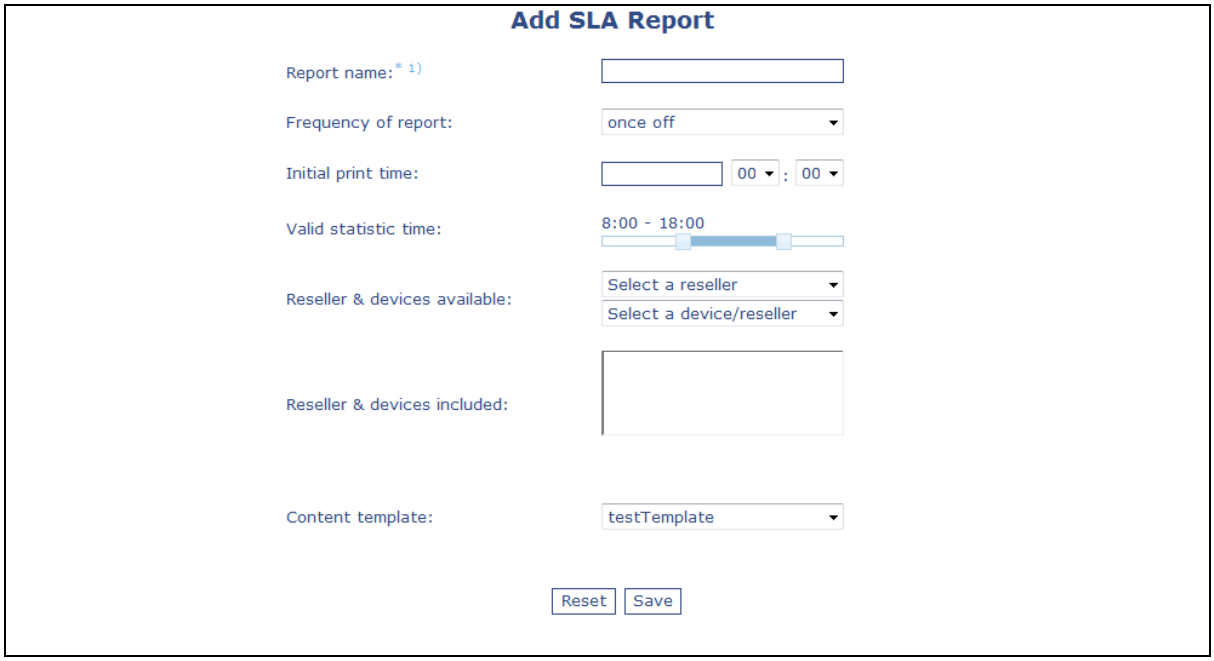


Figure 127: The add SLA report page

Enter the relevant parameters.

Parameter	Description	Options
Report Name	Name of report	
Frequency of report	How often a report is generated	once off, hourly, daily or weekly
Initial print time	Initial start time	
Valid statistic time	Window of time to report	0 – 24 hours
Reseller & devices available	To select resellers and devices	From Monitor database
Reseller & devices included	Display added resellers or devices	
Content template	Content template that report is based on	

Table 38: Parameters for adding an SLA report

The figure below shows an example of a SLA report with two devices.

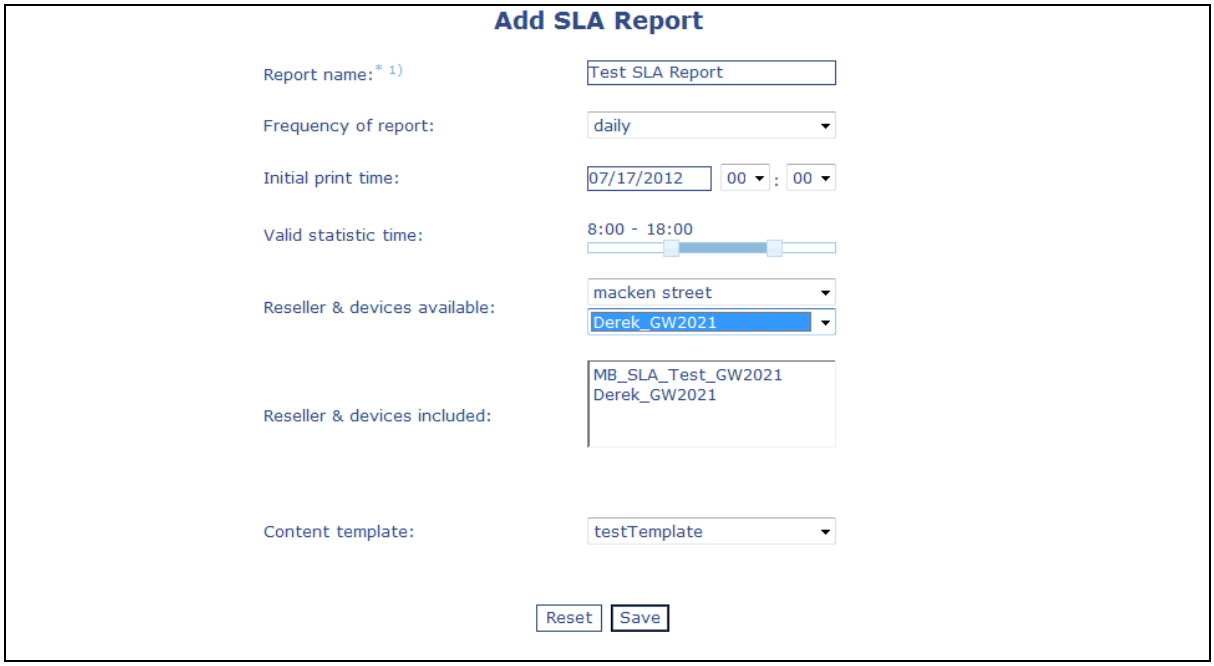


Figure 128: An example SLA report showing two devices

Note: for this report two routers have been added. When you have configured the SLA Report, Monitor will periodically access the router, every hour, and initiate a 'create scheduled task' on a router. This task tells a router to upload SLA statistics to Monitor. If Monitor is unable to schedule a task a due to an outage, it will attempt to connect again to a router when the connection is back up.

35.4 Viewing an SLA report

To view an SLA report, access any router on Monitor that has been added to the SLA report.

Click **SLA Reporting**.

Select the relevant report in the drop down menu and select a date.

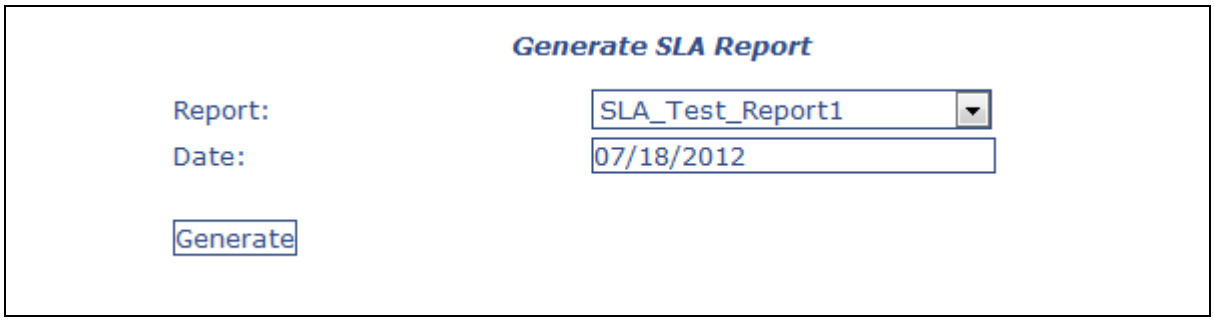


Figure 129: The generate SLA report page

Click **Generate** and the report will open.

Report: SLA_Test_Report1

(Date 18/7/2012 Hours of operation: 08:00 - 19:00)

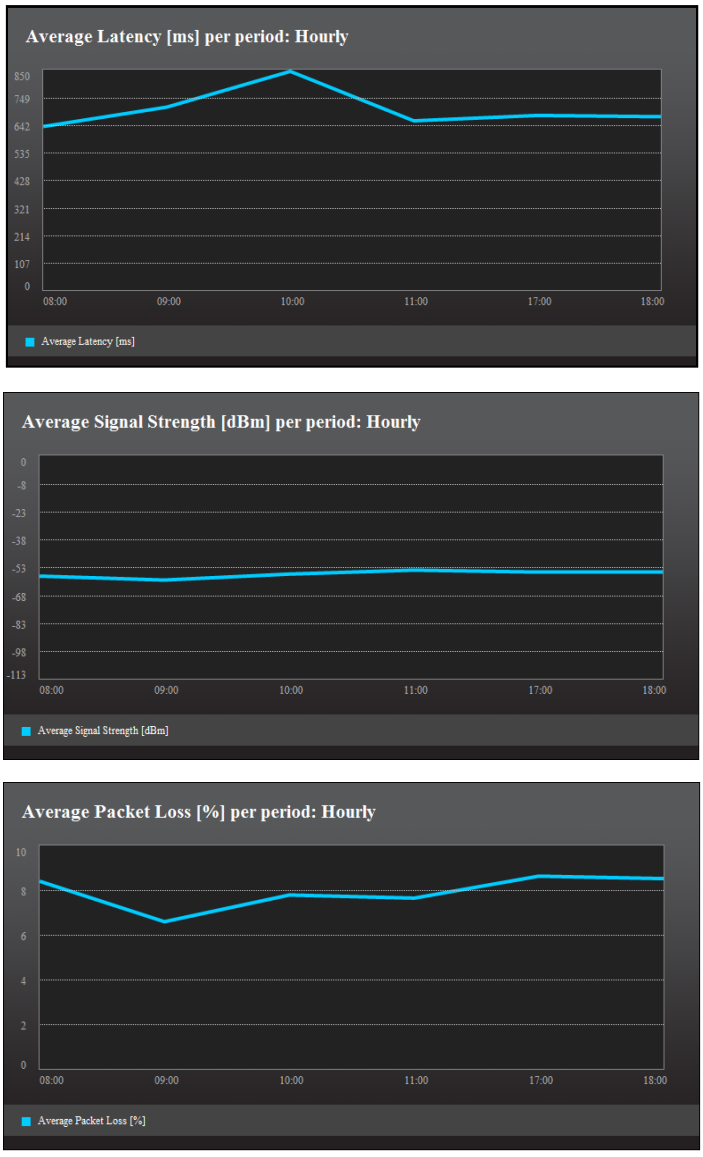


Figure 130: Example of SLA report output

35.5 Viewing automated SLA reports

An automated version of this report is stored in the database and you can access it through any router assigned to the report.

To view these reports access any router assigned to the report.

Select the **relevant report**. A list of downloadable PDFs appears.

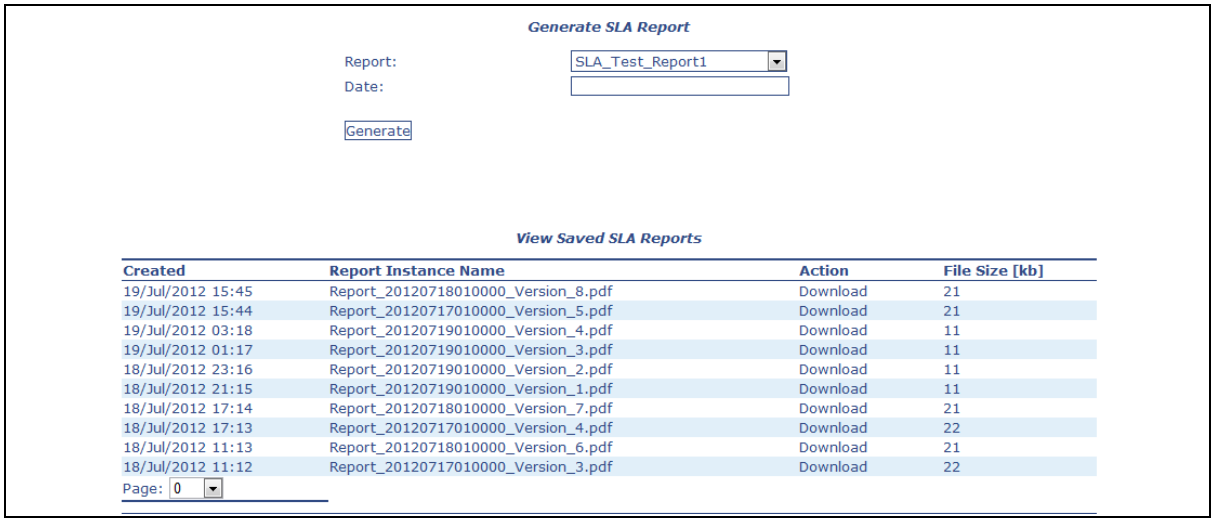


Figure 131: Example of an automated report

To view a report, click **Download** in the report's row. A PDF version of the report appears.

35.6 Configuring router upload protocol

The protocol the router uses to upload the files is set for each device on Monitor.

Edit a device and from the Activator upload protocol drop-down menu, select the desired protocol and enter in the relevant TFTP Server Address and then enter the TFTP Server Port number to match.

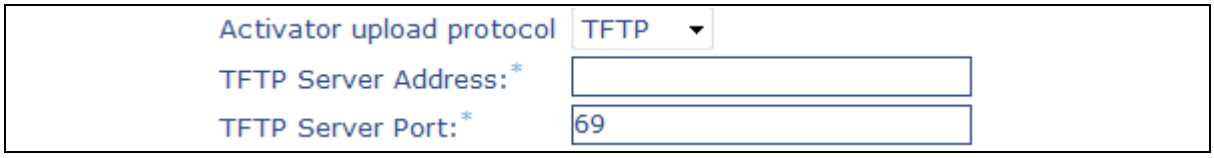


Figure 132: The upload protocol parameters

36 Configuring SLA for a router

SLA reporting works in two parts:

- The Virtual Access Monitor system server connects via SSH into the router and schedules the task of uploading statistics to Monitor.
- The Virtual Access router monitors UDP keepalive packets. It creates and stores statistics in bins. These statistics are uploaded every hour to the Monitor server.

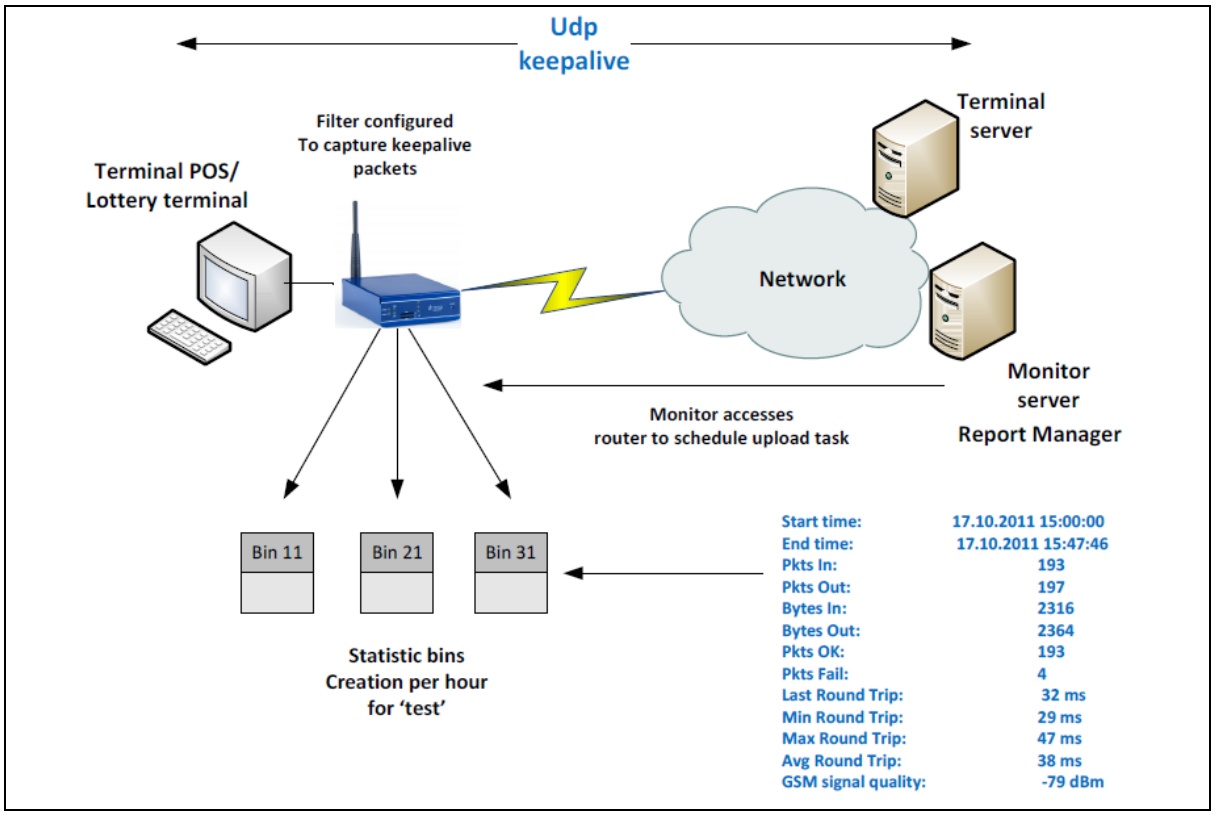


Figure 133: The SLA function

This section describes how to configure SLA on a router. For information on how to configure Monitor for SLA reporting read the previous section 'Configuring SLA on Monitor'.

36.1 Configuring SLA for a router via the web interface

Login to the web interface using your login credentials.

In the top menu, select **Services -> SLA Daemon**. The SLA Daemon page appears.

Figure 134: The SLA daemon page

In the Basic Settings section, click **Add**. The basic settings section for SLA Daemon appears.

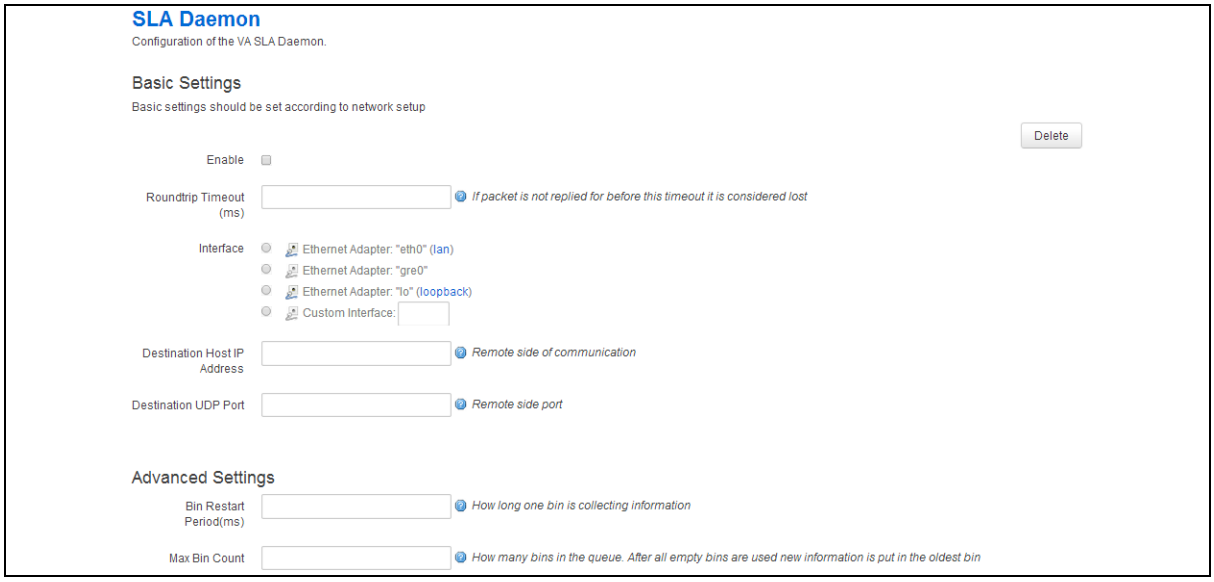

SLA Daemon
Configuration of the VA SLA Daemon.
Basic Settings
Basic settings should be set according to network setup
Delete
Enable
Roundtrip Timeout (ms)
If packet is not replied for before this timeout it is considered lost
Interface
Ethernet Adapter: "eth0" (lan)
Ethernet Adapter: "gre0"
Ethernet Adapter: "lo" (loopback)
Custom Interface:
Destination Host IP Address
Remote side of communication
Destination UDP Port
Remote side port
Advanced Settings
Bin Restart Period(ms)
How long one bin is collecting information
Max Bin Count
How many bins in the queue. After all empty bins are used new information is put in the oldest bin

Figure 135: The SLA daemon page

Check **Enable**.

In the Timeout for Roundtrip Timeout field, type in a time.

Select an interface on which traffic should be monitored.

Specify a destination IP address for the keepalive packets that are originated on the LAN.

Specify a destination UDP port for the keepalive packets that are originated on the LAN.

Scroll down to the Advanced Settings section.

In the Bin Restart Period field, type in a bin collection time.

In the Max Bin count field, type the maximum number of Bins stored on a router.

Name	Type	Required	Default	Description
Enable	Check box	Yes	none	Enables SLAD daemon.
Roundtrip Timeout (ms)	integer	Yes	None	Specifies the time in milliseconds that a packet is not replied before this timeout

				expires it is considered as lost.
Interface	Radio button menu	Yes	None	Specifies the interface on which traffic should be monitored.
Destination Host IP Address	IPv4 address	Yes	None	Specifies the destination IP address for the keepalive packets that are originated on the LAN.
Destination UDP port	Integer	Yes	None	Specifies the destination UDP port.
Bin Restart Period (ms)	Integer	Yes	None	Specifies how long one bin is collecting information.
Max Bin Count	Integer	Yes	None	Specifies how many bins are in the queue. After all empty bins are used, new information is put in the oldest bin.

When you have made all your configuration changes, click **Save & Apply**.

36.2 Configuring SLA for a router via UCI interface

You can also configure SLA UCI through CLI using UCI command suite.

The configuration file is stored at:

/etc/config/slad

To view the configuration file, enter:

```
uci export slad
```

or

```
uci show slad
```

```
uci export slad
package slad
config slad 'main'
        option enable 'yes'
        option roundtrip_timeout_msec '5000'
        option interface 'lan'
        option destination_host_ip_address '10.1.1.2'
        option destination_udp_port '53'
        option bin_restart_period_msec '3600000'
        option max_bin_count '73'
uci show slad
slad.main=slad
```

```
slad.main.enable=yes
slad.main.roundtrip_timeout_msec=5000
slad.main.interface=lan
slad.main.destination_host_ip_address=10.1.1.2
slad.main.destination_udp_port=53
slad.main.bin_restart_period_msec=3600000
slad.main.max_bin_count=73
```

36.3 SLA statistics

Type the command line `sla` to show all available statistic options.

```
root@GW1021:~# sla
sla [ current ] | [ all ] | [ oldest ] | [ newest ] | [newest N] | [ range: YYYYMMDDHH-YYYYMMDDHH ]
root@GW1021:~#
```

Figure 136: Output from the command line sla

Option	Description
current	Shows current sla bin
all	Shows all bin stored on the router
oldest	Shows the oldest sla bin stored
newest	Shows two newest valid bins
newest N	Shows the newest valid bin
range YYYYMMDDHH-YYYYMMDDHH	Shows all bins that match specified time range

Type the command `sla current` to show current statistics.

```
root@GW1021:~# sla current
---------------------------------
Bin valid:              No
Start time:             01.01.1970 03:34:00
End time:               n/a
Pkts In:                1
Pkts Out:               1
Bytes In:               15
Bytes Out:              15
Pkts OK:                1
Pkts Fail:              0
Last Round Trip:        1 ms
Min Round Trip:         1 ms
Max Round Trip:         1 ms
Avg Round Trip:         1 ms
Min GSM signal quality: n/a
Max GSM signal quality: n/a
Avg GSM signal quality: n/a
Availability:           100.00%
```

Figure 137: Output from the command line sla current

Type the command `sla newest` to show the newest statistics.

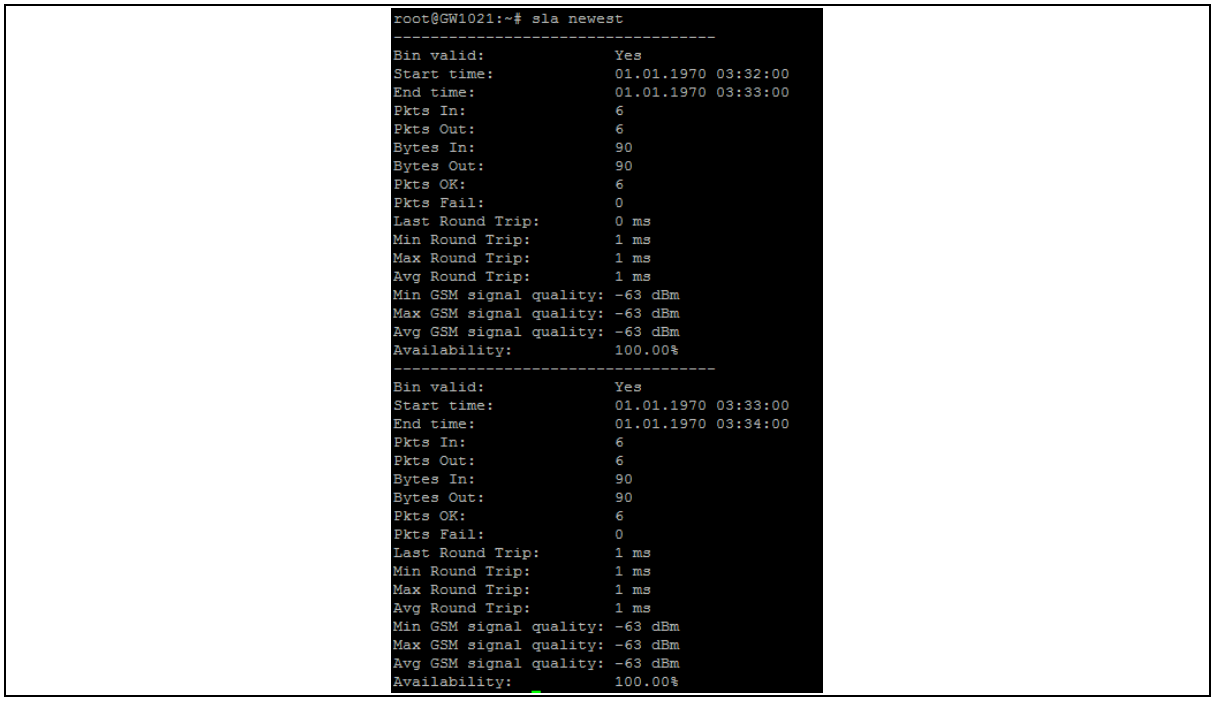

root@GW1021:~# sla newest
Bin valid: Yes
Start time: 01.01.1970 03:32:00
End time: 01.01.1970 03:33:00
Pkts In: 6
Pkts Out: 6
Bytes In: 90
Bytes Out: 90
Pkts OK: 6
Pkts Fail: 0
Last Round Trip: 0 ms
Min Round Trip: 1 ms
Max Round Trip: 1 ms
Avg Round Trip: 1 ms
Min GSM signal quality: -63 dBm
Max GSM signal quality: -63 dBm
Avg GSM signal quality: -63 dBm
Availability: 100.00%
Bin valid: Yes
Start time: 01.01.1970 03:33:00
End time: 01.01.1970 03:34:00
Pkts In: 6
Pkts Out: 6
Bytes In: 90
Bytes Out: 90
Pkts OK: 6
Pkts Fail: 0
Last Round Trip: 1 ms
Min Round Trip: 1 ms
Max Round Trip: 1 ms
Avg Round Trip: 1 ms
Min GSM signal quality: -63 dBm
Max GSM signal quality: -63 dBm
Avg GSM signal quality: -63 dBm
Availability: 100.00%

Figure 138: Output from the command line sla newest

37 Diagnostics

37.1 ADSL diagnostics

37.1.1 ADSL PPPoA connections

To check the status of an ADSL line, in the top menu, select **Status -> ADSL Status**. The ADSL Status page appears.

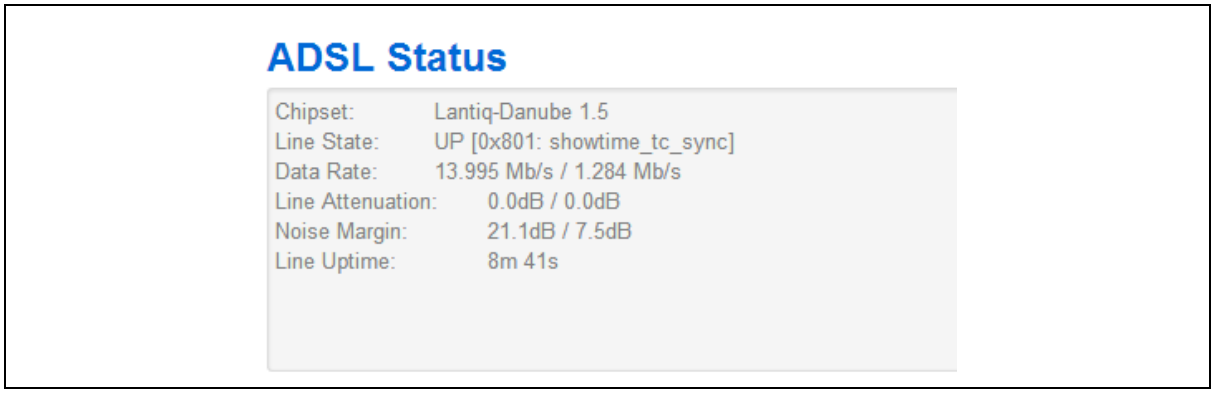

ADSL Status
Chipset: Lantiq-Danube 1.5
Line State: UP [0x801: showtime_tc_sync]
Data Rate: 13.995 Mb/s / 1.284 Mb/s
Line Attenuation: 0.0dB / 0.0dB
Noise Margin: 21.1dB / 7.5dB
Line Uptime: 8m 41s

Figure 139: The ADSL status page

To check an IP address, transmit and received counter on an ADSL interface, in the top menu, select **Network -> Interfaces**. The Interface Overview page appears.

Figure 140: The interfaces overview page

37.1.2 ADSL PPPoEoA connections

To check the status of an ADSL line, in the top menu, select **Status -> ADSL Status**. The ADSL Status page appears.

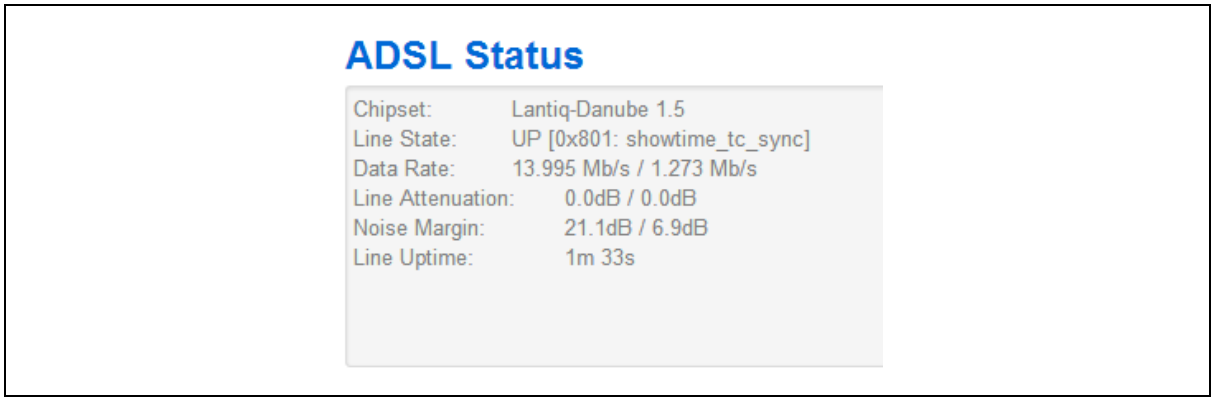

ADSL Status
Chipset: Lantiq-Danube 1.5
Line State: UP [0x801: showtime_tc_sync]
Data Rate: 13.995 Mb/s / 1.273 Mb/s
Line Attenuation: 0.0dB / 0.0dB
Noise Margin: 21.1dB / 6.9dB
Line Uptime: 1m 33s

Figure 141: The ADSL status page

To check an IP address, transmit and received counter on an ADSL interface, in the top menu, select **Network -> Interfaces**. The Interface Overview page appears.

Figure 142: The interfaces overview page

37.1.3 ADSL bridge connections

To check the status of an ADSL line, in the top menu, select **Status -> ADSL Status**. The ADSL Status page appears.

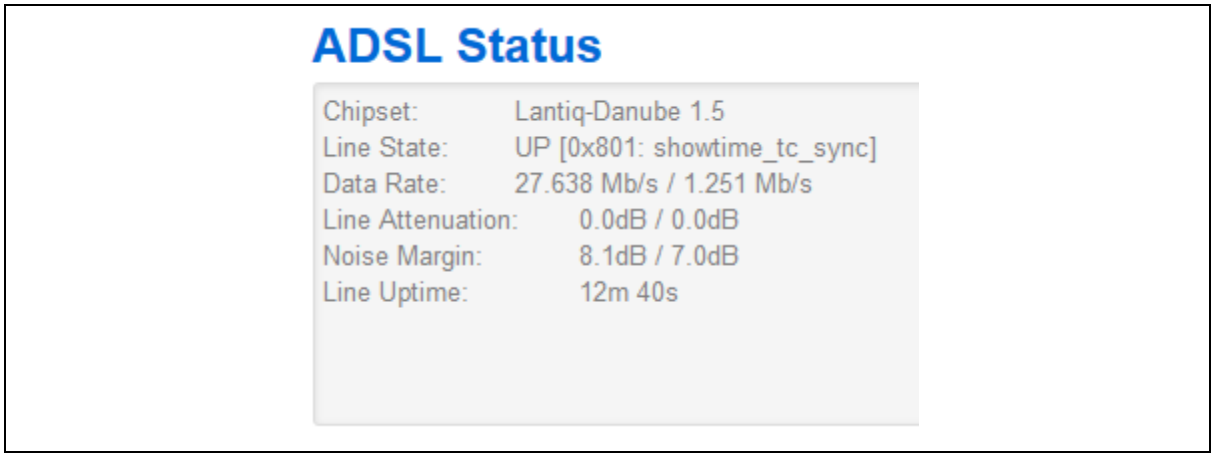

ADSL Status
Chipset: Lantiq-Danube 1.5
Line State: UP [0x801: showtime_tc_sync]
Data Rate: 27.638 Mb/s / 1.251 Mb/s
Line Attenuation: 0.0dB / 0.0dB
Noise Margin: 8.1dB / 7.0dB
Line Uptime: 12m 40s

Figure 143: The ADSL status page

To check an IP address, transmit and received counter on an ADSL interface, in the top menu, select **Network -> Interfaces**. The Interface Overview page appears.

Figure 144: The interfaces overview page

37.2 ALL diagnostics

The ‘va5420_stats /dev/ttyLC0’ command provides statistical information about the operation of the interface. Here an example:

```
root@VA_router:~# va5420_stats /dev/ttyLC0
TRANSMIT STATS
        tx bytes                566600
        tx buffer full counts   0
        tx underruns            0
        tx discards             0

RECEIVE STATS
        rx bytes                566988
        rx overruns             0
        rx discards             0

V.23 MODE STATS
        rx bytes                0
        tx bytes                0
        rx samples              0
        tx samples              0
        rx carrier on           0
        tx carrier on           0
```

You can set the statistical information using ‘va5420_stats_reset /dev/ttyLC0’.

The example below shows the command ‘va5420_status /dev/ttyLC0’; it displays status information about the device.

```
root@VA_router:~# va5420_status /dev/ttyLC0
Mode:           Transparent
Wire mode:      2-wire
PCM Encoding:   A-Law
```

37.3 Automatic operator selection diagnostics via the web interface

37.3.1 Checking the status of the Multi-WAN package

When interfaces are auto created they are presented in the network and in the Multi-WAN package.

To check interfaces created in the Multi-WAN package, from the top menu, select **Network -> Multi-WAN**.

To check interfaces that have been created in the network package, from the top menu, select **Network -> Interfaces**.

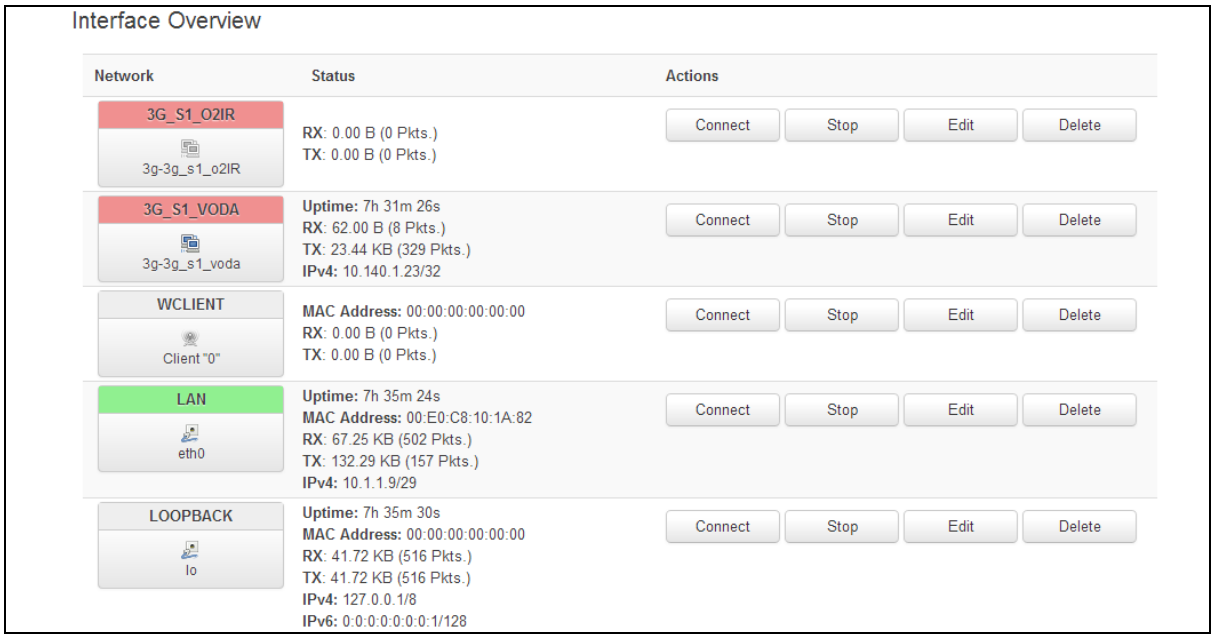


Figure 145: The interface overview page

To check the status of the interface you are currently using, in the top menu, click **Status**. The Interface Status page appears.

Scroll down to the bottom of the page to view Multi-WAN Stats.

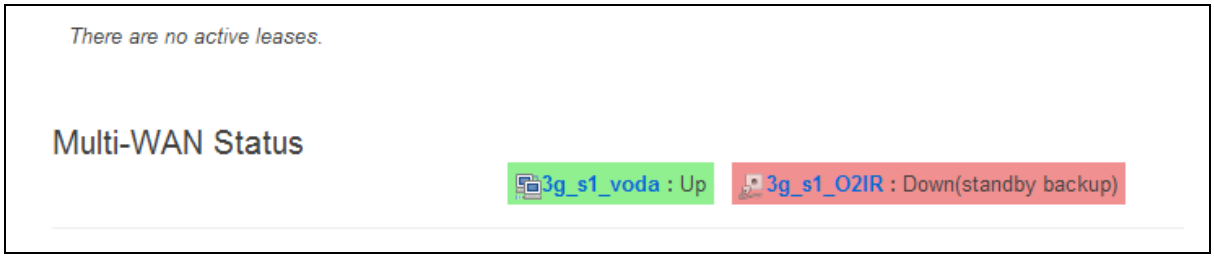


Figure 146: The status page: multi-WAN status section page

37.4 Automatic operator selection diagnostics via UCI

To check interfaces created in the multi-WAN package, enter:

```
cat /var/const_state/multiwan
```

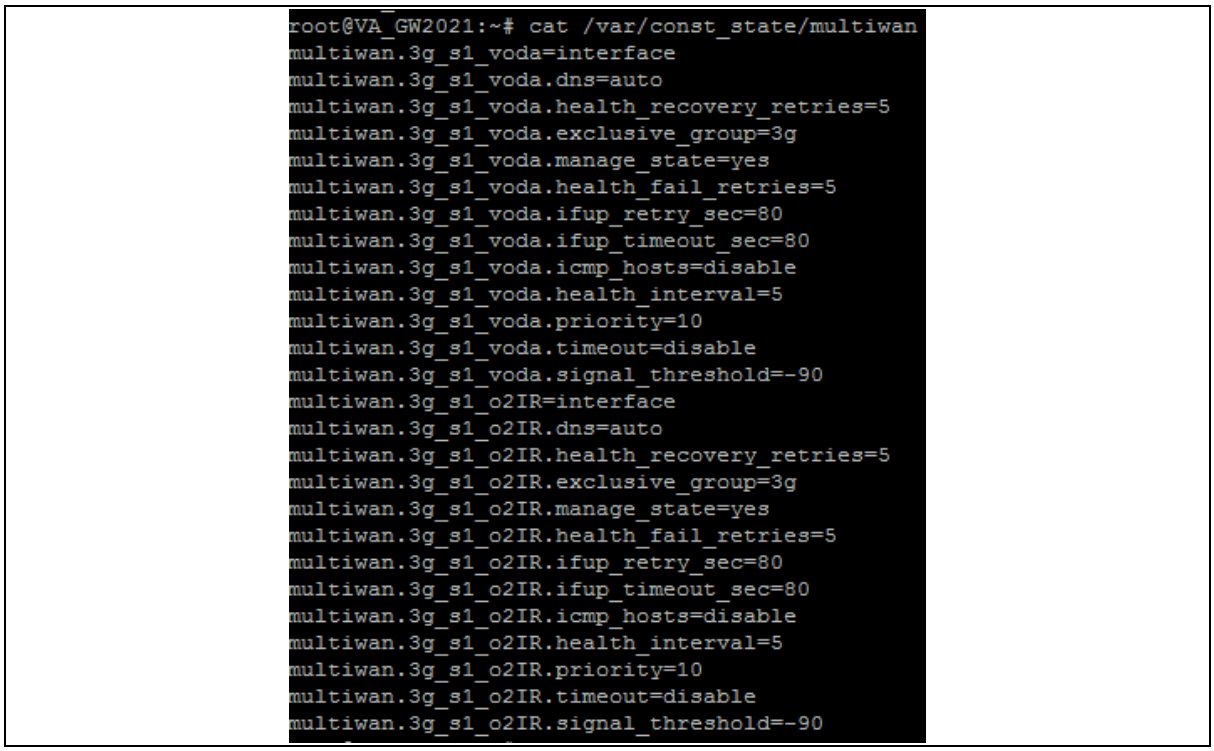


Figure 147: Output from the command: cat /var/const_stat/multiwan

To check interfaces created in the network package, enter:

```
cat /var/const_state/network
```

```
root@VA_GW2021:~# cat /var/const_state/network
network.3g_s1_voda=interface
network.3g_s1_voda.auto=no
network.3g_s1_voda.service=umts
network.3g_s1_voda.roaming_sim=1
network.3g_s1_voda.defaultroute=no
network.3g_s1_voda.username=internet
network.3g_s1_voda.apn=hs.vodafone.ie
network.3g_s1_voda.operator=vodafone IE
network.3g_s1_voda.proto=3g
network.3g_s1_voda.sim=1
network.3g_s1_voda.password=internet
network.3g_s1_o2IR=interface
network.3g_s1_o2IR.auto=no
network.3g_s1_o2IR.service=umts
network.3g_s1_o2IR.roaming_sim=1
network.3g_s1_o2IR.defaultroute=no
network.3g_s1_o2IR.username=internet
network.3g_s1_o2IR.apn=hs.vodafone.ie
network.3g_s1_o2IR.operator=o2 IRL
network.3g_s1_o2IR.proto=3g
network.3g_s1_o2IR.sim=1
network.3g_s1_o2IR.password=internet
root@VA_GW2021:~#
```

To check the status of the interface you are currently using, enter:

```
cat /var/const_state_/mobile
```

```
root@VA_GW2021:~# cat /var/const_state/mobile
mobile.3g_0=status
mobile.3g_0.sim1_iccid=89314404000039480265
root@VA_GW2021:~#
root@VA_GW2021:~#
root@VA_GW2021:~# cat /var/state/mobile
mobile.3g_0=status
mobile.3g_0.sim_slot=1
mobile.3g_0.sim_in=yes
mobile.3g_0.registered=5, Roaming
mobile.3g_0.reg_code=5
mobile.3g_0.imei=357784040034322
mobile.3g_0.imsi=204043726270034
mobile.3g_0.registered_pkt=5, Roaming
mobile.3g_0.reg_code_pkt=5
mobile.3g_0.area=BCC
mobile.3g_0.tech=2
mobile.3g_0.technology=UTRAN
mobile.3g_0.operator=1,0,"vodafone IE",2
mobile.3g_0.cell=AA787
mobile.3g_0.sig_dbm=-113
root@VA_GW2021:~#
```

Figure 148: Output from the command cat /vat/const_state_/mobile

37.5 CESoPSN diagnostics

CESoPSN uses one package - cesopd. To view the CESoPSN configuration:

```
root@VA_router:~# # uci export cesopd

package cesopd

config cesopd 'main'
        option log_severity '5'
        option enable '1'

config port 'Port1'
        option enable '1'
        option devname 'ttyLC0'
        …..
```

The cesop command provides several options to investigate the operation of the CESoPSN service. The output provided by these commands will allow the Virtual Access support team to assist you.

```
cesop show all - show all
cesop show config - show configuration
cesop show status - show status
cesop show stats - show statistics
cesop clear stats - clear statistics
```

37.5.1 cesop show config

To show the currently running configuration, enter:

```
root@VA_router:~# cesop show config
Main Config
-----------
enable                        : 1
nodaemon                      : 0
debug_enabled                 : 0
log_severity                  : 5
schedule_mode                 : 1
```

```
schedule_priority             : 10


Port 1 config
--------------------
cardType                      : Single AAL card
enable                        : 1
clock_recovery_enabled        : 1
clock_recovery_debug          : 0
remote_loopback               : 0
udp_local_ipaddr              : 0.0.0.0
udp_local_port                : 5152
udp_remote_ipaddr             : 10.1.42.63
udp_remote_port               : 5152
rtp_payload_type              : 96
packetization_latency         : 5
rx_jitter_buffer_enabled      : 0
rx_jitter_buffer_size_ms      : 24
app_bit_reverse               : 0
app_rx_shift                  : 0
devname                       : ttyLC0
bypass                        : 0
local_loopback                : 0
dce                           : 1
rate                          : 64000
ext_clock                     : 0
fifo_irq_level                : 1
bit_reverse                   : 0
dte_tt_inv                    : 0
dce_tclk_inv                  : 0
dce_rclk_inv                  : 0
x21_clk_invert                : 0
x21_data_delay                : 0
x21_use_vco                   : 0
all_four_wire_mode            : 0
all_pcm_encoding              : alaw
all_rx_attenuator_enabled     : 1
all_rx_analogue_gain_enabled  : 0
```

© Virtual Access 2015

```
all_tx_analogue_loss_enabled  : 0
all_rx_digital_gain           : 0
all_tx_digital_loss           : 0
tdm_intvl_ms                  : 2
```

37.5.2 cesop show status

To show the current operating configuration, enter:

```
root@VA_router:~# cesop show status
Clock status
------------
clockRecHwPresent      1
dacOutputVoltage       1661174
lastFscCount           14195832
Port 1 protocol status
----------------------
remoteIpAddress        10.1.42.63
remotePort             5152
rxPayloadType          96
rxSegmentSize          40
rxSsrc                 451d
rxLBit                 0
rxRBit                 0
rxMBits                0
rxTdmPayload           [D5][D5]...
txPayloadType          96
txSegmentSize          40
txSsrc                 89298337
txLBit                 0
txRBit                 0
txMBits                0
txTdmPayload           [D5][D5]...
```

37.5.3 cesop show stats

To view statistical information about the CESoPSN service, enter cesop show stats.

```
root@VA_router:~# cesop show stats
Port 1 serial statistics
------------------------
reads        476840
readEmpties  0
readFails    0
writes       476889

writeFails   0
writeShorts  0
txBytes      19075560
rxBytes      19075560
Port 1 UDP statistics
---------------------
txFrames      476889
txBytes       26705784
txFails       0
rxFrames      476889
rxBytes       26705784
rxFails       0
rxAddressErrs 0

Port 1 Protocol statistics
--------------------------
rxHeaderErrs 0
rxOutOfOrder 0
rxTdmLenErrs 0
txTdmLenErrs 0

Clock recovery statistics
-------------------------
packetLossCount  0
clockChanges     90
```

37.5.4 cesop clear stats

To reset the statistical counters, enter `cesop clear stats`

```
root@VA_router:~# cesop clear stats
```

cesopd stats cleared.

37.6 DMVPN diagnostics

In the top menu, click **Status -> IPSec**. The IPSec Connections page appears.

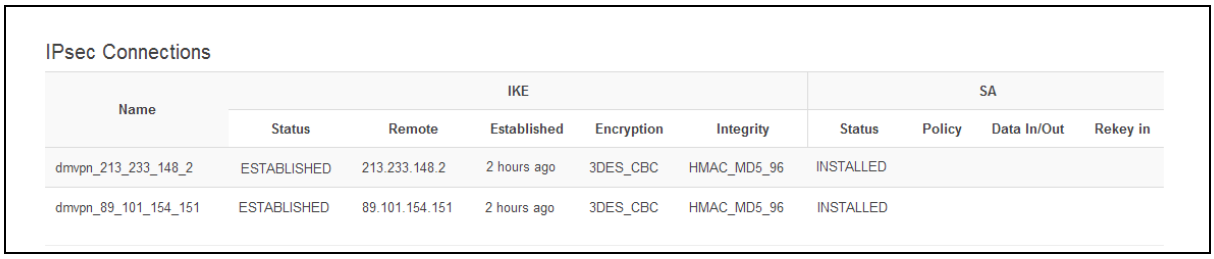


Figure 149: The IPSec connections page

In the Name column, the syntax contains the IPSec Name defined in package dmvpn and the remote IP address of the hub, or the spoke separated by an underscore; for example, dmvpn_213.233.148.2.

To check the status of DMVPN, in the top menu, click **Status -> DMVPN**.

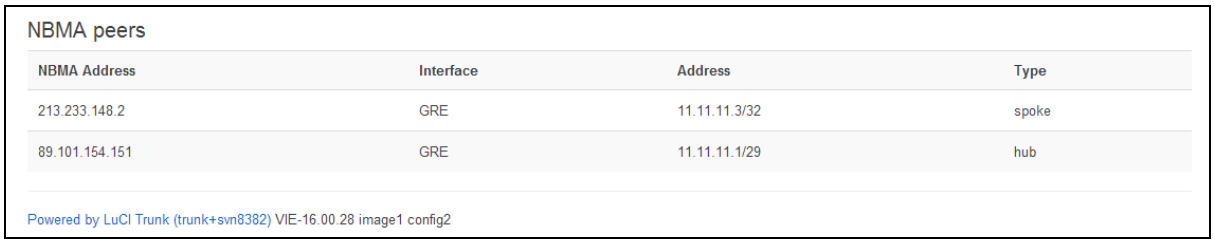


Figure 150: The NBMA peers page

NBMA Address	Interface	Address	Type
Public IP address of the peer.	Interface name	Tunnel IP address of remote node.	Spoke is presented if it is reachable. Hub is known regardless of its reachability. There are two hub statuses 'hub' and 'dead hub'.

Table 39: NBMA peers columns and their descriptions

You can check IPSec status using uci commands.

```
root@GW202x:~# ipsec status
Security Associations (1 up, 0 connecting):
dmvpn_89_101_154_151[1]: ESTABLISHED 2 hours ago,
10.68.234.133[10.68.234.133]...89.101.154.151[89.101.154.151]
dmvpn_89_101_154_151{1}:  REKEYING, TRANSPORT, expires in 55 seconds
dmvpn_89_101_154_151{1}:   10.68.234.133/32[gre] === 192.168./32[gre]
dmvpn_89_101_154_151{1}:  INSTALLED, TRANSPORT, ESP in UDP SPIs: cca7b970_i
d874dc90_o
dmvpn_89_101_154_151{1}:   10.68.234.133/32[gre] === 89.101.154.151/32[gre]
```

You can check DMVPN status using uci commands.

```
:~# opennhrpctl show
Status: ok

Interface: gre-GRE
Type: local
Protocol-Address: 11.11.11.7/32
Alias-Address: 11.11.11.3
Flags: up

Interface: gre-GRE
Type: local
Protocol-Address: 11.11.11.3/32
Flags: up

Interface: gre-GRE
Type: cached
Protocol-Address: 11.11.11.2/32
NBMA-Address: 178.237.115.129
NBMA-NAT-OA-Address: 172.20.38.129
Flags: used up
Expires-In: 0:18
Interface: gre-GRE
Type: static
Protocol-Address: 11.11.11.1/29
```

© Virtual Access 2015

```
NBMA-Address: 89.101.154.151
Flags: up
```

The above command output is explained in the table below.

Interface	**Interface name taken from package network**
Type	incomplete: Resolution request sent. negative: Negative cached. cached: Received/relayed resolution reply. shortcut_route: Received/relayed resolution for route. dynamic: NHC registration. dynamic_nhs: Dynamic NHS from dns-map. static: Static mapping from config file. dynamic_map: Static dns-map from config file. local_route: Non-local destination, with local route. local_addr: Local destination (IP or off-NBMA subnet)
Protocol-Address	Tunnel IP address
NBMA-Address	Pre-NAT IP address if NBMA-NAT-OA-Address is present or real address if NAT is not present.
NBMA-NAT-OA-Address	Post NAT IP address. This field is present when Address is translated in the Network.
Flags	up: Can send all packets (registration ok) unique: Peer is unique. used: Peer is in kernel ARP table. lower-up: opennhrp script executed successfully.
Expires-In	Expiration time.

37.7 File system diagnostics

The standard Linux directories on such as /bin, /etc, /usr are in a ramdisk. Any changes you make to them will be lost on reboot.

Store anything that needs to survive reboot in flash.

There is a UBIFS (flash) file system mounted on /etc. Configuration files, keys and certificates are stored there so that they survive reboot. Normally it is not necessary to store any other files in flash. One exception, for example, is a banner file for logins.

37.8 Firewall diagnostics

The routers OS relies on netfilter for packet filtering, NAT and mangling. The UCI Firewall provides a configuration interface that abstracts from the iptables system to provide a simplified configuration model that is fit for most regular purposes while enabling the user to supply needed iptables rules on his own when needed.

The firewall section is its own package located within /etc/config/firewall.

Below is an example of a firewall section.

```
root@VA_router:~# uci export /etc/config/firewall
package firewall

config defaults
        option syn_flood '1'
        option input 'ACCEPT'
        option output 'ACCEPT'
        option forward 'ACCEPT'
config zone
        option name 'lan'
        option network 'lan'
        option input 'ACCEPT'
        option forward 'ACCEPT'
        option output 'ACCEPT'
        option family 'any'
        option conntrack '0'

config zone
        option name 'wan_interface'
        option network ' wan_interface'
        option masq '1'
        option mtu_fix '1'
        option forward 'ACCEPT'
        option output 'ACCEPT'
        option family 'any'
        option conntrack '0'
        option input 'ACCEPT'
```

```
config forwarding
        option src 'lan'
        option dest 'wan_interface'
        option family 'any'

config rule
        option name 'Allow-DHCP-Renew'
        option src 'wan_interface'
        option proto 'udp'
        option dest_port '68'
        option target 'ACCEPT'
        option family 'ipv4'

config rule
        option name 'allow dns'
        option src 'wan_interface'
        option proto 'tcp'
        option dest_port '53'
        option target ' ACCEPT'
        option family 'ipv4'

config rule
        option name 'Allow-Ping'
        option src 'wan_interface'
        option proto 'icmp'
        option target 'ACCEPT'
        option family 'ipv4'
        list icmp_type 'echo-request'

config rule
        option name 'SNMP-trap'
        option src 'wan_interface'
        option proto 'udp'
        option dest_port '162'
        option target 'ACCEPT'
        option family 'ipv4'
```

```
config rule
        option name 'Allow-DHCPv6'
        option src 'wan_interface'
        option src_ip 'fe80::/10'
        option src_port '547'
        option proto 'udp'
        option dest_ip 'fe80::/10'
        option dest_port '546'
        option target 'ACCEPT'
        option family 'ipv6'

config rule
        option name 'Allow-ICMPv6-Input'
        option src 'wan_interface'
        option proto 'icmp'
        option target 'ACCEPT'
        option family 'ipv6'
        option limit '1000/sec'
        list icmp_type 'echo-request'
        list icmp_type 'echo-reply'
        list icmp_type 'destination-unreachable'
        list icmp_type 'packet-too-big'
        list icmp_type 'time-exceeded'
        list icmp_type 'bad-header'
        list icmp_type 'unknown-header-type'
        list icmp_type 'router-solicitation'
        list icmp_type 'neighbour-solicitation'

config rule
        option name 'Allow-ICMPv6-Forward'
        option src 'wan_interface'
        option proto 'icmp'
        option dest '*'
        option target 'ACCEPT'
        option family 'ipv6'
        option limit '1000/sec'
        list icmp_type 'echo-request'
```

```
        list icmp_type 'echo-reply'
        list icmp_type 'destination-unreachable'
        list icmp_type 'packet-too-big'
        list icmp_type 'time-exceeded'
        list icmp_type 'bad-header'
        list icmp_type 'unknown-header-type'
```

To view the available firewall commands, enter:

```
root@VA_router:~# /etc/init.d/firewall
Syntax: /etc/init.d/firewall [command]
```

Available commands:

```
        start   Start the service
        stop    Stop the service
        restart Restart the service
        reload  Reload configuration files (or restart if that fails)
        enable  Enable service autostart
        disable Disable service autostart
```

37.8.1 IP tables

To add a quick firewall rule for dropping packets to a specific IP, enter:

```
root@VA_router:~# iptables -I OUTPUT -d 8.8.8.8/32 -p icmp -j  DROP
```

To disable the rule, enter:

```
root@VA_router:~# iptables -D OUTPUT 1
```

37.8.2 Debug

It is possible to view the iptables commands generated by the firewall program. This is useful if you want to track down iptables errors during firewall restarts or to verify the outcome of certain UCI rules.

To see the rules as they are executed, run the fw command with the FW_TRACE environment variable set to 1:

```
root@VA_router:~# FW_TRACE=1 fw reload
```

To direct the output to a file for later inspection, enter:

```
root@VA_router:~# FW_TRACE=1 fw reload 2>/tmp/iptables.log
```

37.9 GPS diagnostic commands

You can use the utility GPS to run diagnostic commands against the GPSD application.

When you run GPS at the command prompt without parameters, it prints the menu listing all available commands.

For example to view the last known router position, enter gpspeek:

```
root@Demo:~# gpspeek
Fix: 3D,1423135517,53.342546,-6.241331,23.800000,223.700000,0.000000,nan
```

37.10 Interfaces diagnostics

37.10.1 Interfaces status

To show the current running interfaces, enter:

```
root@VA_router:~# ifconfig
3g-CDMA   Link encap:Point-to-Point Protocol
          inet addr:10.33.152.100  P-t-P:178.72.0.237  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1400  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:428 (428.0 B)  TX bytes:2986 (2.9 KiB)


eth0      Link encap:Ethernet  HWaddr 00:E0:C8:12:12:15
          inet addr:192.168.100.1  Bcast:192.168.100.255
Mask:255.255.255.0
          inet6 addr: fe80::2e0:c8ff:fe12:1215/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6645 errors:0 dropped:0 overruns:0 frame:0
          TX packets:523 errors:0 dropped:0 overruns:0 carrier:0
```

```
          collisions:0 txqueuelen:1000
          RX bytes:569453 (556.1 KiB)  TX bytes:77306 (75.4 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:385585 errors:0 dropped:0 overruns:0 frame:0
          TX packets:385585 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:43205140 (41.2 MiB)  TX bytes:43205140 (41.2 MiB)
```

To display a specific interface enter: `ifconfig <name>`:

```
root@VA_router:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:E0:C8:12:12:15
          inet addr:192.168.100.1  Bcast:192.168.100.255
Mask:255.255.255.0
          inet6 addr: fe80::2e0:c8ff:fe12:1215/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7710 errors:0 dropped:0 overruns:0 frame:0
          TX packets:535 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:647933 (632.7 KiB)  TX bytes:80978 (79.0 KiB)
```

37.10.2 Route status

```
root@VA_router:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use
Iface
192.168.100.0   *               255.255.255.0   U     0      0        0
eth0
```

A route will only be displayed in the routing table when the interface is up.

37.10.3 Mobile status

To display information and status of mobile interfaces like 4G or CDMA, enter:

```
root@VA_router:~# cat /var/state/mobile
mobile.3g_1_1_1=status
mobile.3g_1_1_1.auto_info=/etc/3g_1-1.1.auto
mobile.3g_1_1_2=status
mobile.3g_1_1_2.auto_info=/etc/3g_1-1.2.auto
mobile.3g_1_1_1.sim_slot=1
mobile.3g_1_1_1.sim_in=yes
mobile.3g_1_1_1.imsi=240016005892879
mobile.3g_1_1_1.registered=1, Home network
mobile.3g_1_1_1.reg_code=1
mobile.3g_1_1_1.registered_pkt=1, Home network
mobile.3g_1_1_1.reg_code_pkt=1
mobile.3g_1_1_1.area=FFFE
mobile.3g_1_1_1.cell=189150A
mobile.3g_1_1_1.tech=7
mobile.3g_1_1_1.technology=E-UTRAN
mobile.3g_1_1_1.operator=0,0,"Vodafone",7
mobile.3g_1_1_1.sim1_iccid=89460127120912066226
mobile.3g_1_1_2.sim_slot=1
mobile.3g_1_1_2.sim_in=yes
mobile.3g_1_1_2.operator="Vodafone"
mobile.3g_1_1_2.cdma_roaming=Not Roaming
mobile.3g_1_1_2.cdma_roaming_code=0
mobile.3g_1_1_2.cdma_srvmode=EVDO Rev B
mobile.3g_1_1_2.cdma_srvmode_code=5
mobile.3g_1_1_2.cdma_total_drc=0.0 kbps
mobile.3g_1_1_2.cdma_carr_cnt=2
mobile.3g_1_1_2.cdma_rx0=78
mobile.3g_1_1_2.sig_dbm=nan
mobile.3g_1_1_2.cdma_rx1=105
```

37.10.4 ADSL status

The ADSL chipset has its own subset of commands.

```
root@VA_router:~# /etc/init.d/dsl_control
Syntax: /etc/init.d/dsl_control [command]
```

Available commands:

```
        start   Start the service
        stop    Stop the service
        restart Restart the service
        reload  Reload configuration files (or restart if that fails)
        enable  Enable service autostart
        disable Disable service autostart
        status  Get DSL status information
        lucistat  Get status information in lua friendly format
```

To view the current status of the ADSL interface, enter:

```
root@VA_router:~# /etc/init.d/dsl_control status
Chipset:                Lantiq-Danube 1.5
Line State:             UP [0x801: showtime_tc_sync]
Data Rate:              2.280 Mb/s / 291 Kb/s
Line Attenuation:       6.3dB / 3.3dB
Noise Margin:           31.1dB / 35.9dB
Line Uptime:            2d 18h 8m 30s
```

To restart the ADSL interface, enter:

```
root@VA_router:~# /etc/init.d/dsl_control restart
```

37.11 ISDN pseudowire diagnostics

37.11.1 Packages

ISDN pseudowire uses two packages: Asterisk and LCR.

To view configuration of the LCR package, enter:

```
root@VA_router:~# uci export lcr
package lcr

config lcr 'main'
        option enable '1'
        list msn '384740'
        list msn '384741'
```

To view configuration of the asterisk package, enter:

```
root@VA_router:~# uci export asterisk
package asterisk

config provider
        option host '10.1.183.20'
        option hostport '5060'
        option username 'username'
        option secret 'secret'

config client
        option username 'username'
        option secret 'secret'
        option msn '384720'

config client
        option username 'username'
        option secret 'secret'
        option 384721
```

37.11.2 Asterisk CLI diagnostics

You can use Asterisk CLI to view diagnostics. To enter `asterisk CLI`:

```
root@VA_router:~# asterisk -r
```

To view configured SIP peers when in asterisk CLI, enter:

```
root@VA_router:~# sip show peers
Name/username  Host            Dyn Forcerport ACL Port        Status
VA_username    10.1.23.15      N               5060           Unmonitored
1 sip peers [Monitored: 0 online, 0 offline Unmonitored: 1 online, 0
offline]
```

To view current call diagnostics when in asterisk CLI, enter:

```
root@VA_router:~# sip show channels stats
Peer        Call ID      Duration      Recv: Pack Lost (     %)      Jitter
Send: Pack  Lost (     %)      Jitter
10.1.23.15  4abaa449705  00:00:08     0000000426 0000000000 ( 0.00%) 0.0000
0000000391 0000000000 ( 0.00%) 0.0002
1 active SIP channel
```

To exit asterisk CLI, enter:

```
~# exit
```

37.11.3 ISDN LED status

The ISDN port has two LEDs indicating the status of the audio channels in use.

ISDN top LED	On	Audio channel is up (dial tone or call in progress)
	Off	Audio channel is inactive
ISDN bottom LED	On	Audio channel is up (dial tone or call in progress)
	Off	Audio channel is inactive

37.12 IPSec diagnostics

Virtual Access routers use the strongSwan package for IPSec.

To view IPSEC configuration on the router, enter:

```
root@VA_router:~# uci export strongswan
```

To restart strongSwan, enter:

```
root@VA_router:~# etc/init.d/strongswan restart
```

To view IPSEC status, enter:

```
root@VA_router:~# ipsec statusall
```

To view a list of IPSEC commands, enter:

```
root@VA_router:~# ipsec –help
```

37.13 Multi-WAN diagnostics

The multi-WAN package is an agent script that makes multi-WAN configuration simple, easy to use and manageable. It comes complete with load balancing, failover and an easy to manage traffic ruleset. The uci configuration file/etc/config/multiwan is provided as part of the multi-WAN package.

The multi-WAN package is linked to the network interfaces within /etc/config/network.

Note: multi-WAN will not work if the WAN connections are on the same subnet and share the same default gateway.

To view the multi-WAN package, enter:

```
root@VA_router:~# uci export /etc/config/multiwan
package multiwan

config multiwan 'config'
        option enabled 'yes'
        option preempt 'yes'
        option alt_mode 'no'

config interface 'ADSL'
        option health_interval '10'
        option icmp_hosts 'dns'
        option timeout '3'
        option health_fail_retries '3'
        option health_recovery_retries '5'
        option priority '1'
        option manage_state 'yes'
        option exclusive_group '0'
        option ifup_retry_sec '300'
        option ifup_timeout_sec '40'

config interface 'Ethernet'
        option health_interval '10'
        option icmp_hosts 'dns'
        option timeout '3'
        option health_fail_retries '3'
        option health_recovery_retries '5'
```

```
        option priority '2'
        option manage_state 'yes'
        option exclusive_group '0'
        option ifup_retry_sec '300'
        option ifup_timeout_sec '40'
```

The following output shows the multi-WAN standard stop/start commands for troubleshooting.

```
root@VA_router:~# /etc/init.d/multiwan
Syntax: /etc/init.d/multiwan [command]

Available commands:
        start   Start the service
        stop    Stop the service
        restart Restart the service
        reload  Reload configuration files (or restart if that fails)
        enable  Enable service autostart
        disable Disable service autostart
```

When troubleshooting, make sure that the routing table is correct using route –n.

Ensure all parameters in the multi-WAN package are correct. The name used for multi-WAN must be identical, including upper and lowercases, to the actual ADSL interface name defined in your network configuration.

To check the names and settings are correct, browse to **Network - > interfaces** or alternatively, run: **cat / etc / config / network** through CLI.

Enter the name of the WAN interface to configure, and then click **Add**. The new section for configuring specific parameters will appear.

37.14 PAD diagnostics

37.14.1 Showing Log

The modules will write events to the log if they are configured to do so.

To see the event that are already logged, type the following at the command prompt: **logread**.

The log contains the events of many modules. To filter a specific module, type **logread | grep module_name**, for example, if you want to see the vald events enter:

```
logread -f | grep vald
```

Note: the vald module has a command that enables the logging of the payload.When enabled, vald will additionally log the payload of all received and sent packets.

To enable payload logging, enter:

```
root@VA_router:~# val trace on
val trace enabled
```

Logread as a '-f' option that output the events as the log grows. It is very useful when you want to live trace. You may use it this way:

```
root@VA_router:~# logread –f
```

or

```
root@VA_router:~# logread -f
```

37.14.2 Debugging guidelines

If you are having trouble configuring PAD, use the list below to debug.

Is the router receiving calls?	To check the router is receiving calls, look at the log and search for an event similar to the following: Nov 28 13:05:40 VA_router user.debug vald: (1): Incoming VC, TCP accepted, VC id 0, LCN 4095
Is data being received on the asynchronous serial?	To check data is being received on the asynchronous serial, enter: **tserv show stats**. TERMINAL 4, Dev: /dev/ttySC3 State: CONNECTED Serial Bytes Rx (2036) Tx (26624) TxErrs (0) TCP Packets Rx (23) Tx (16) TxErrs (0) TCP Bytes Rx (26624) Tx (2036) UDP Datagrams Rx (0) Tx (0) TxErrs (0) UDP Bytes Rx (0) Tx (0) DSR Up (0) Down (0) Uptime 0 hrs 0 mins 22 secs For more details refer to section 6, 'Terminal Server'.
Are the vald, padd and tservd modules running?	To check if the modules are running, follow the instructions described in the PAD section. For more details refer to the 'Terminal Server' section in this manual.

Is the Terminal Server connected to padd?	To check if the Terminal Server is connected to padd, look at the log and check the Terminal Server status. For more details refer to the 'Terminal Server' section in this manual.
Is the Terminal Server detecting the serial cable?	To check if the Terminal Server is detecting the serial cable, enter: **tserv show serial**. For more details refer to the 'Terminal Server' section in this manual.
Is the padd port connected to the good vald?	Check in the configuration that the padd port to be used is connected to the good vald port. The connection is created by the link_id parameter of the padd configuration file.
Is the vald port used correctly configured?	Check the configuration of the port in the vald configuration file. Check that the IP address and TCP port match the ones used by the VAL peer.

37.15 Terminal Server diagnostics

You can check Terminal server application diagnostics by using the commands described below.

```
root@VA_router:~# tserv
=== Termserv disgnostics. Command syntax: ===

tserv show stats - show statistics
tserv clear stats - clear statistics
tserv show serial - show serial interface status
tserv send serial0 <data>- send data to serial port 0
tserv start capture N, N=port number (0 to 3) - start capturing rx serial data
tserv print capture N, N=port number (0 to 3) - print captured rx serial data
tserv show serial txlog-hex <Port> [length], Port=port cfg index (0 to 3), length=length to show
tserv show serial rxlog-hex <Port> [length], Port=port cfg index (0 to 3), length=length to show
tserv show serial txlog-asc <Port> [length], Port=port cfg index (0 to 3), length=length to show
tserv show serial rxlog-asc <Port> [length], Port=port cfg index (0 to 3), length=length to show
tserv show debug - show debug info
```

```
tserv show userial stats - show USB serial card statistics
tserv clear userial stats - clear USB serial card statistics
tserv start userial rxlog <Port> - start USB serial card rx log
tserv show userial rxlog <Port> <offs> <length> - show USB serial card rx
log
tserv show userial version <Port> - show USB serial card firmware version
tserv show userial cpld status <Port> - show USB serial card CPLD
programming status
tserv upgrade userial - initiate upgrade of the USB serial card
tserv quit - terminate termserv process
```

Note: tservd process has to be running otherwise diagnostics options for terminal server will not be available.

37.16 VRRP diagnostics

Two available diagnostic options exist: via web interface and command line.

37.16.1 VRRP diagnostics web interface

To see VRRP through the web interface, in the top menu, select Status -> Status. The VRRP status settings appear.

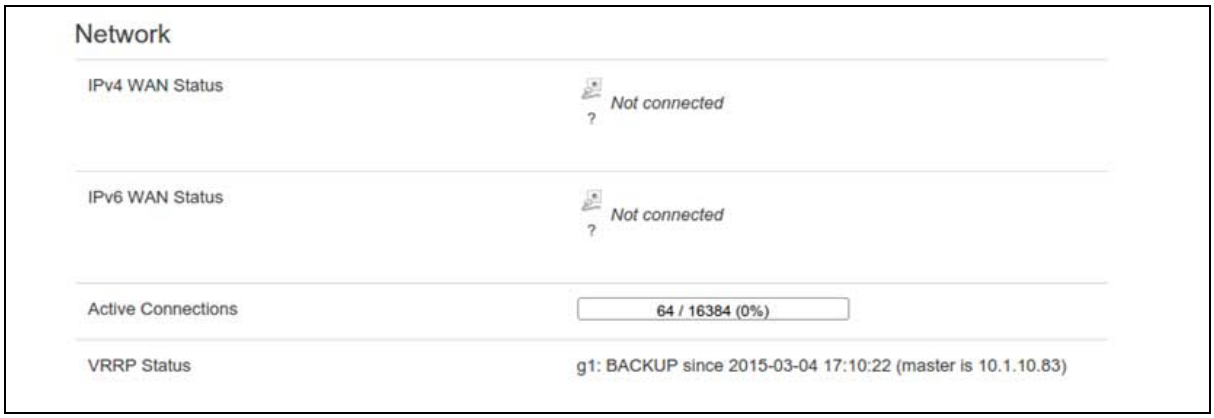


Figure 151: The VRRP status settings

37.16.2 VRRP diagnostics using the command line interface

To view VRRP using the CLI interface, SSH into the router and enter:

```
cat /var/state/vrrp command
vrrp.g1.state=BACKUP
vrrp.g1.masterip=10.1.10.83
vrrp.g1.timestamp=1425489022
```

37.17 Diagnostics for WiFi AP mode

To check for any hosts associated with WiFi AP, in the top menu, select **Network -> WiFi**. The Wireless Overview page appears.

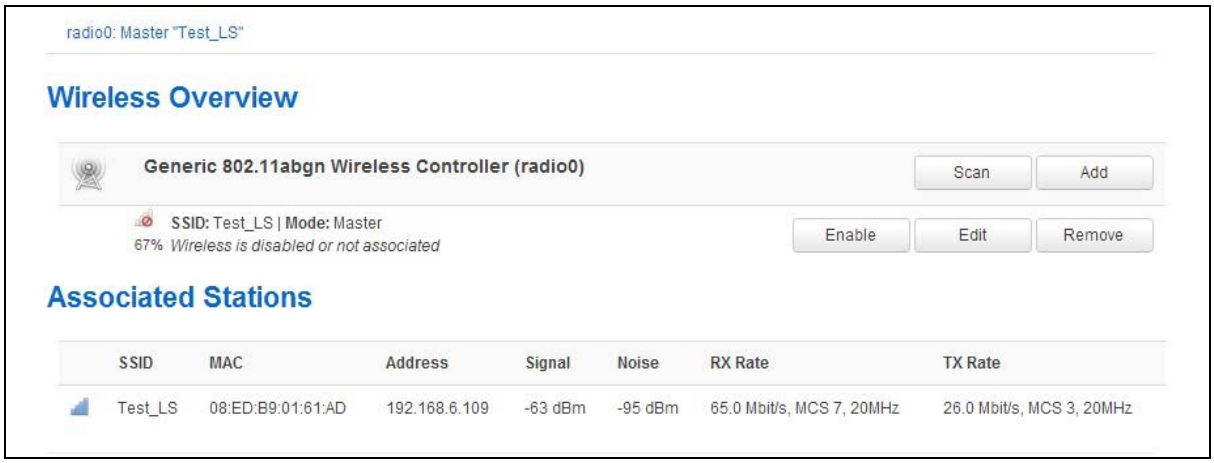


Figure 152: The wireless overview page showing associated hosts

37.18 Diagnostics for WiFi client mode

To check for connectivity, in the top menu, select **Network -> Interfaces**. The WCLIENT interface will show receive and transmit packets and an IP address.

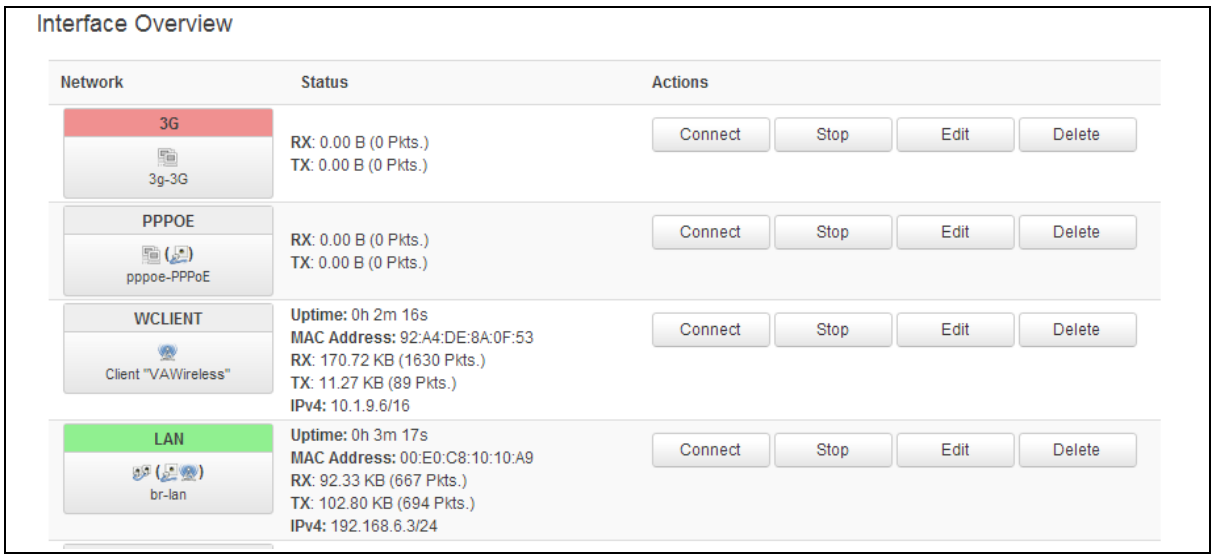


Figure 153: The interface overview page showing WClient stats